مبادئ الجبر المجرد

الدكتور
محمد عبد العظيم سعود
أستاذ الرياضيات البحتة
كلية العلوم بجامعة عين شمس

بسم الله الرحمن الرحيم

توطئة

اللهم اجعل هذا العمل من ذلك الذى لا ينقطع برحيل أصحابه ، مفيداً لقرائه ، وبعد ؛

فأقدم هذا الكتاب من عميق إحساسى بلزوم تكوين مكتبة علمية بلسان عربى ، يكون عوناً لأبناء أمتنا العربية على استيعاب مبادئ علم الجبر ، الذى تمتد جذوره إلى ما أسسه الأجداد فى ماضينا السحيق ، أيام أن كانت لهم الريادة فى شتى العلوم والمعارف.

هو كتاب تعليمى ، بيد أن أفكار المادة العلمية عميقة إلى حدٍ ما ، ولهذا حرصت على أن تكون البراهين واضحة جلية ، فاستطردت كثيراً فى شرحها وتبيانها ، على غير مألوف أغلب الكتب المتقدمة ، فلم أترك لفطنة القارئ إلا القليل ، بل ربما أقل القليل . فكنت أتخير البراهين من مختلف الكتب والمراجع بمقياسى الإبداع والوضوح فى آن ، ثم أزيد الأمر وضوحاً إن لزم ذلك.

وأما عن قضية المصطلح فقد أصبح لزاماً على بعد أن آثرت استخدام مفردة "مجموعة" ترجمة لمفردة "set" فى كتاب سابق لى كان بعنوان "**أسس الجبر والجبر الخطى**" أن استخدم مفردة " زمرة " هنا ترجمة لمفردة " group " وهذا هو الشأن فى كل بلداننا العربية التى شاهدتها، على النقيض مما آثرناه هنا فى مصر ، وكنت ميالاً إليه . فكان أساتذتنا الأجلاء يستخدمون مفردة " فئة " ترجمة لكلمة " set " ، "مجموعة" ترجمة لكلمة "group ".

واستخدمت مفردة "هومومورفيزم" الاستخدامين المتاحين فصرفتها مرات وقلت "هومومورفيزماً" ومنعتها من الصرف تارات وقلت " هومومورفيزم" فى موضع النصب، وكلا الرأيين النحويين صائب عند أصحابه. وقل مثل هذا فى "مونومورفيزم" و "إبيمورفيزم" ، و"أيزومورفيزم" و"إندومورفيزم" و"أوتومورفيزم" كذلك. وقد استخدمت كثيراً مفردة "تشاكل" ترجمة لكلمة " أيزومورفيزم ". واستخدمت الرمزين γ_n ، S_n للتعبير عن الزمرة المتماثلة من الرتبة n ، فقد جاء كلاهما فى الكتب والكلاسيكيات. وفعلت الشىء ذاته حيث استخدمت $\mathbb{Z}/n\mathbb{Z}$ ، $\mathbb{Z}_n$ للتعبيرعن نفس الزمرة ، فبينما يكون الرمز الثانى أشيع فى الكتب الإنجليزية والأمريكية ، نرى – جُلّ – أو كُلّ الكتب الألمانية

تستخدم الرمز الأول . وعبرت عن تركيب الراسمين (أو الدالتين) f ، g أحياناً بـ Pog وأحياناً fg إلا إذا التبس الأمر بين التركيب والضرب فلزم التنويه . كما أوضحت بالبرهان الشكلى (formal proof) أن لا فرق بين الكتابة f والكتابة f(X) ، فكلتاهما تصلح تعبيراً عن راسم (أو دالة) فاستخدمت كلتيهما .

والكتاب مُترع بالأمثلة المحلولة ، وليست كلها مختلفة الفكر ، كما أنها ليست جميعاً بالطبع فى نفس المستوى الذهنى . وأنصح للقارئ هنا ألا يسترسل فى قراءتها ، بل عليه أن يتوقف بعد قليل منها ، ليحاول حل باقيها ، ومقارنة حله بالحل المثبت بالكتاب ، للتعرف على مواطن القصور فى حله ، إن كان ثمة قصور .

والمادة العلمية فى هذا الكتاب تغطى ما يدرس بالفرقتين الثالثة والرابعة بكليات العلوم والتربية فى جامعاتنا العربية – والمصرية بعضها – وأكبر الظن أنها تزيد . هو يعرض للزمر (groups) ، الحلقات (rings) ، الحقول (fields) ، ويختم بنظرية جالوا (Golois Theory)

أود فى النهاية أن أشكر لدار الكتب العلمية للنشر والتوزيع ، وعلى رأسها صاحبها ومديرها الأستاذ محمد محمود الحماسة لإخراج هذا الكتاب.

وعلى بركة الله

محمد عبد العظيم سعود

1 Group Theory نظرية الزمر

القسم



١-١ الربط وأشباه الزمر Compositions and Semigroups

١-١-١ تعريف : لتكن M مجموعة غير خالية

(أ) الراسم من M × M الى M يسمى ربطاً فى M (عملية على M أو تركيباً فى M)

(ب) الربط $M \times M \to M$: . يقال له

$$(a,b) \mapsto a.b$$

تشاركي (إدماجي أو تجميعي) (associative) إذا كان $(a.b).c = a.(b.c)$ لجميع $a,b,c \in M$

إبدالى (commutative) إذا كان : $a.b = b.a$ لجميع $a,b \in M$.

١-١-٢ تعريف : لتكن M مجموعة غير خالية ، وليكن

$$.: M \times M \to M$$
$$(a,b) \mapsto a.b$$

لكل $a \in M$ الراسمان :

$$\ell_a : M \to M \quad , \quad r_a : M \to M$$
$$x \mapsto a.x \qquad\qquad x \mapsto x.a$$

يسميان النقل الأيمن والنقل الأيسر (على الترتيب) لـــ $(M,.)$ حول a

(right translation, resp. left translation about a)

١-١-٣ ملحوظة : الربط "." فى M يكون تشاركياً (إدماجياً ، تجميعياً) إذا كان وفقط

إذا كان : $\ell_{a.b} = \ell_a o \ell_b \quad : \quad \forall a,b \in M$

البرهان :

$$\forall a,b \in M \quad : \quad \ell_{a.b} = \ell_a o \ell_b$$
$$\Leftrightarrow \quad \forall a,b,c \in M \ : \ \ell_{a.b}(c) = (\ell_a o \ell_b)(c)$$
$$\Leftrightarrow \quad \forall a,b,c \in M \ : \ (a.b).c = \ell_a(\ell_b(c))$$
$$= \ell_a(b.c)$$
$$= a.(b.c)$$

١-١-٤ تعريف : لتكن H مجموعة غير خالية ، وليكن "." ربطاً تشاركياً (تجميعياً ، إدماجياً) فى H . عندئذ فإن الزوج $(H,.)$ يسمى **شبه زمرة** (Semigroup) .

١-١-٥ تعريف : لتكن $(H,.)$ شبه زمرة . يقال للعنصر $e\in H$ إنه **عنصر محايد أيسر** (left neutral element) لـ $(H,.)$ إذا كان وفقط إذا كان : لكل $a\in H$: $e.a=a$.
ويقال إنه **عنصر محايد أيمن** (right neutral element) لـ$(H,.)$ إذا كان وفقط إذا كان : لكل $a\in H$: $ae=a$. ويقال للعنصر $e\in H$ إنه **عنصر محايد** (neutral element) لـ$(H,.)$، إذا كان وفقط إذا كان عنصراً محايداً أيمن وعنصراً محايداً أيسر لـ$(H,.)$.

١-١-٦ ملحوظة : شبه الزمرة $(H,.)$ لها على الأكثر عنصر محايد واحد .

البرهان : ليكن e، e' عنصرين محايدين لشبه الزمرة $(H,.)$. عندئذ فإن :

$$e = e.e' = e'$$

e عنصر محايد e' عنصر محايد

١-١-٧ تعريف : لتكن $(H,.)$ شبه زمرة ، ولها العنصر المحايد e . يقال إن b **معكوس أيسر** (left inverse) (**معكوس أيمن** (right inverse)) على الترتيب لـ$a\in H$ إذا كان (وفقط إذا كان) $b.a=e$ $(a.b=e)$ على الترتيب .

١-١-٨ أمثلة :

مثال ١ : $\mathbb{N}:\{0,1,2,...\}$ مجموعة الأعداد الطبيعية . ولتكن

$$+:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$$
$$(m,n)\mapsto m+n$$

عملية الجمع العادية. $(\mathbb{N},+)$ شبه زمرة ولها العنصر المحايد "0" . هذا واضح لأن :

$$\forall m,n,\ell\in\mathbb{N}:(m+n)+\ell=m+(n+\ell),$$
$$\forall m\in\mathbb{N}:\quad 0+m=m=m+0$$

(يقال لشبه الزمرة التي لها عنصر محايد إنها **مونويد** (monoid)) .

مثال ٢ : لتكن M مجموعة غير خالية وليكن Map(M) مجموعة جميع الرواسم من M إلى M. وليكن :

$$o:Map(M)\times Map(M)\to Map(M)$$
$$(f,g)\to fog$$

تركيب الرواسم . عندئذ فإن $(Map(M),o)$ شبه زمرة وعنصرها المحايد id_M راسم الوحدة على M. هذا واضح لأن :

$$\forall f,g,h \in Map(M) : (fog)oh = fo(goh),$$
$$\forall f \in Map(M) : id_M of = f = fo\ id_M$$

<u>مثال ٣</u> : ليكن $n>1$ عدداً طبيعيا وليكن $M_{n\times n}(\mathbb{R})$ مجموعة جميع المصفوفات من النوع $n\times n$ وعناصرها (مداخلها (entries)) كلها أعداد حقيقية . الراسمان :

$$\begin{aligned} * : M_{n\times n}(\mathbb{R})\times M_{n\times n}(\mathbb{R}) &\to M_{n\times n}(\mathbb{R}) \\ (A,B) &\mapsto AB+BA \end{aligned}$$

$$\begin{aligned} \widehat{*} : M_{n\times n}(\mathbb{R})\times M_{n\times n}(\mathbb{R}) &\to M_{n\times n}(\mathbb{R}) \\ (A,B) &\mapsto AB-BA \end{aligned}$$

(AB يعنى ضرب المصفوفات العادى)

ليسا تشاركيين (إدماجيين ، تجميعيين) .

<u>البرهان</u> : ليكن

$$C := \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\ ,\ B := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\ ,\ A := \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

$$(A*B)*C - A*(B*C) = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} - \begin{pmatrix} 2 & 4 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ -1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

كذلك فإن :

$$(A\,\widehat{*}\,B)\,\widehat{*}\,C - A\,\widehat{*}\,(B\,\widehat{*}\,C) = \begin{pmatrix} -2 & 2 \\ 1 & 2 \end{pmatrix} - \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

<u>مثال ٤</u> : ليكن

$$H := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{R} \right\}$$

$$. : H\times H \to H$$

عملية الضرب العادية للمصفوفات. عندئذ فإن $(H,.)$ شبه زمرة (لأن ضرب المصفوفات عملية تشاركية (إدماجية ، تجمعية)) .

ولكل $x\in\mathbb{R}$ يكون $\begin{pmatrix}1 & x\\ 0 & 0\end{pmatrix}$ عنصراً محايداً أيسر لـ $(H,.)$ ، لأن :

$$\begin{pmatrix}1 & x\\ 0 & 0\end{pmatrix}\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}$$

بينما $(H,.)$ ليس لها أى عنصر محايد أيمن ، لأنه بافتراض أن $\begin{pmatrix}x & y\\ 0 & 0\end{pmatrix}$ عنصر محايد أيمن لها فإن :

$$\forall a,b\in\mathbb{R}:\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\begin{pmatrix}x & y\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\Rightarrow\begin{pmatrix}ax & ay\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}$$

$$\Rightarrow\quad \forall a,b\in\mathbb{R}: ax=a, ay=b$$

وهذا مستحيل .

١-٢ الزمر Groups

١-٢-١ تعريف : لتكن G مجموعة غير خالية ، $.:G\times G\to G,\ (a,b)\to ab$ عملية . تسمى $(G,.)$ **زمرة** إذا تحقق :

(أ) $\forall a,b,c\in G:(a.b).c=a.(b.c)$

(ب) $\exists e\in G\quad \forall a\in G:\quad e.a=a$

(جـ) $\forall a\in G\ \exists\, b\in G: b.a=e$

سنكتب عادة G بدلاً من $(G,.)$ ، وسنكتب ab بدلاً من a.b

١-٢-٢ ملحوظات :

لتكن G زمرة ، e معرفة كما فى (١-٢-١)

(أ) $\forall a,b\in G:\ \ ab=e\Rightarrow ba=e$

(ب) e هو عنصر محايد فى G ومن ثم (١-١-٦) فإنه وحيد .

(جـ) $\forall a\in G\quad \exists_1 b\in G$ ($b\in G$ يوجد واحد بالضبط) $:ba=e$.

يسمى b **معكوس** a (inverse)، وسنعبر عن معكوس a بـــ a^{-1} .

(د) $\forall a,b \in G: \quad (ab)^{-1} = b^{-1}a^{-1} \,,\; (a^{-1})^{-1} = a$

(هـــ) $\forall a,x,y \in G: \quad ax = ay \Rightarrow x = y$

$xa = ya \Rightarrow x = y$

(و) $\forall a,b \in G \quad \exists_1 x \in G: \quad ax = b \wedge \exists_1 y \in G: ya = b$

(ز) $\forall a \in G: \; \ell_a, r_a$ تناظران أحاديان

البرهان : (أ) ، (ب) متروكان كتمرين للقارئ .

(جـــ) $ba = e \;\wedge\; ca = e \;\Rightarrow\; b = eb = (ca)b = c(ab) \;=\; c(ba) = ce \;=\; c$

(أ)   (ب)

(د) $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = e$. ولأن المعكوس وحيد (من جـــ)

ينتج أن $(ab)^{-1} = b^{-1}a^{-1}$

كذلك فإن :

$$a^{-1}a = e \wedge aa^{-1} = e \Rightarrow aa^{-1} = e \wedge a^{-1}a = e$$

ولأن المعكوس وحيد (من جـــ) ينتج أن $(a^{-1})^{-1} = a$

(هـــ) $ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay) \Rightarrow (a^{-1}a)x = (a^{-1}a)y \Rightarrow ex = ey \Rightarrow x = y$

وبالمثل $xa = ya$.

(و) $x := a^{-1}b$ تحقق المعادلة $ax = b$. إذا كان هناك حل آخر z فإن :

$$az = b \Rightarrow a^{-1}(az) = a^{-1}b \Rightarrow (a^{-1}a)z = a^{-1}b \Rightarrow z = a^{-1}b$$

أى أن الحل $x = a^{-1}b$ وحيد.

وبالمثل $y := ba^{-1}$ حل وحيد للمعادلة $ya = b$.

(ز) إعادة صياغة لـــ (و).

١-٢-٣ تعريف : G زمرة (أو شبه زمرة) . G **إبدالية** (commutative) (abelian) : إذا كان $\forall a,b \in G: \quad ab = ba$

١-٢-٤ ملحوظة : فى حالة الزمر (أشباه الزمر) الإبدالية عادة يكتب $a+b$ بدلاً من $a.b$ ، $-a$ بدلا من a^{-1} على أساس أن العملية هى"+" من حيث الشكل .

١-٢-٥ أمثلة :

مثال ١ : مجموعة الأعداد الصحيحة $\mathbb{Z}$ ، مع عملية الجمع العادية +

$$+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$$
$$(a,b) \to a+b$$

تكون زمرة إبدالية . وهذا واضح لأن :

$$\forall a,b,c \in \mathbb{Z}: \quad (a+b)+c = a+(b+c)$$
$$\exists 0 \in \mathbb{Z} \quad \forall a \in \mathbb{Z}: \quad 0+a = a \ (= a+0)$$

0 هو العنصر المحايد فى $(\mathbb{Z},+)$

$$\forall a \in \mathbb{Z} \quad \exists(-a) \in \mathbb{Z}: \ -a+a = 0 = a+(-a)$$

$-a$ هو معكوس a فى $(\mathbb{Z},+)$

$$\forall a,b \in \mathbb{Z}: \quad a+b = b+a$$

وبالمثل فإن $(\mathbb{Q},+)$ مجموعة الأعداد الكسرية (النسبية) مع عملية الجمع العادية ، $(\mathbb{R},+)$ مجموعة الأعداد الحقيقية مع عملية الجمع العادية ، $(\mathbb{C},+)$ مجموعة الأعداد المركبة مع عملية الجمع للأعداد المركبة كلها تكون زمراً إبدالية .

مثال ٢ : لتكن $\mathbb{R}_+^*$ مجموعة الأعداد الحقيقية الموجبة (أكبر من الصفر) ،

$$. : \mathbb{R}_+^* \times \mathbb{R}_+^* \to \mathbb{R}_+^*$$
$$(a,b) \mapsto a.b$$

عملية الضرب العادية . $(\mathbb{R}_+^*,.)$ تكون زمرة إبدالية لأن :

$$\forall a,b,c \in \mathbb{R}_+^* : (a.b).c = a.(b.c)$$
$$\exists\, 1 \in \mathbb{R}_+^* \quad \forall a \in \mathbb{R}_+^* : \quad 1.a = a (= a.1)$$

1 هو العنصر المحايد

$$\forall a \in \mathbb{R}_+^* \quad \exists\, a^{-1} \in \mathbb{R}_+^* : \quad a^{-1}.a = 1 (= a.a^{-1})$$

a^{-1} هو معكوس a

$$\forall a,b \in \mathbb{R}_+^* : \quad a.b = b.a$$

وبالمثل فإن $(\mathbb{Q}\setminus\{0\},.)$, $(\mathbb{R}\setminus\{0\},.)$, $(\mathbb{C}\setminus\{0\},.)$ تكون زمراً إبدالية .

<u>مثال ٣</u> : لتكن X مجموعة غير خالية، $\gamma(X)$ مجموعة جميع التناظرات الأحادية من X على نفسها . وليكن

$$\begin{array}{rcl} o:\gamma(X)\times\gamma(X) & \to & \gamma(X) \\ (f,g) & \mapsto & fog \end{array}$$

هو تركيب الرواسم .

عندئذ فإن $(\gamma(X),o)$ زمرة . (انظر مثال ٢ فى (١-١-٨)) .

$\begin{array}{rcl} id_X : X & \to & X \\ x & \mapsto & x \end{array}$ تناظر أحادى ، أى أن $id_X \in \gamma(X)$ ، لكل $f\in\gamma(X)$:

$$id_X \circ f = f (= f\circ id_X)$$

أى أن id_X هو العنصر المحايد فى $\gamma(X)$.

لأن $\gamma(X)$ هى مجموعة جميع التناظرات الأحادية من X على نفسها ، عندئذ فإنه لكل $f\in\gamma(X)$ يوجد $f^{-1}\in\gamma(X)$ (معكوس الراسم f) بحيث إن :

$$f^{-1}\circ f = id_X (= f\circ f^{-1})$$

والآن لتكن $X=\{1,2,...,n\}$. سنكتب γ_n للتعبير عن $\gamma(X)$. تسمى γ_n **<u>الزمرة المتماثلة</u>** من الرتبة n ‏(Symmetric Group of Order n) (فى كثير من الكتب يستخدم الرمز S_n بدلاً من γ_n).

عناصر γ_n تسمى **<u>تبديلات</u>** (Permutations) على الأعداد 1 ، 2 ، ... ، n .

<u>اصطلاح</u> : إذا كانت i_1 ، i_2 ، ... ، i_n عناصر المجموعة $X=\{1,2,...,n\}$.

فإننا سنكتب $\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$ للتعبير عن الراسم $\begin{array}{rcl} f:X & \to & X \\ k & \mapsto & i_k \end{array}$

لاحظ أن γ_n ليست إبدالية لـــ $n\geq 3$ ، لأن :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

بينما

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

ولتوضيح طريقة "الضرب" : فى الحالة الثانية $2 \to 1$ ثم $2 \to 2$. إذن $2 \to 1$. $1 \to 2$ ثم $3 \to 1$. إذن $3 \to 2$. وأخيراً $3 \to 3$ ثم $1 \to 3$. إذن $1 \to 3$. فى الحالة الأولى $3 \to 1$ ثم $3 \to 3$. إذن $3 \to 1$. $2 \to 2$ ثم $1 \to 2$. إذن $1 \to 2$. وأخيراً $1 \to 3$ ثم $2 \to 1$. إذن $2 \to 3$.

كثير من الكتب يتبع تعريفاً آخر "للضرب" فيضرب بالكيفية الآتية :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

أى أن $2 \to 1$ ثم $2 \to 2$ فيكون $2 \to 1$ ؛ $1 \to 2$ ثم $3 \to 1$ فيكون $3 \to 2$ ؛ $3 \to 3$ ثم $1 \to 3$ فيكون $1 \to 3$. لكننا آثرنا الطريقة الموضحة لأن عملية الضرب هنا تركيب راسمين .

<u>**طريقة مختصرة للكتابة**</u> : سنوضح هذه الطريقة بالأمثلة الآتية :

التبديلة $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$ تكتب كذلك $(1 \;\; 3 \;\; 5 \;\; 2 \;\; 4)$

أى أن "صورة" 1 هى 3 ، "صورة" 3 هى 5 ، وهكذا ...

التبديلة $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ تكتب : $(1 \;\; 2 \;\; 4)$

(3 لم تظهر لأن "صورة" 3 هى نفسها)

التبديلة $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$ تكتب $(1 \;\; 2)\,(3 \;\; 5)$

(4 لم تظهر لان "صورة" 4 هى 4)

<u>**مثال ٤**</u> : لتكن X مجموعة غير خالية ، G زمرة ، $Map(X,G)$ مجموعة جميع الرواسم من X إلى G . لكل $f,g \in Map(X,G)$ سنعرف $fg \in Map(X,G)$ بالطريقة الآتية :

$$\forall x \in X : \qquad (fg)(x) := f(x)g(x)$$

والآن سنعرف "." العملية فى $Map(X,G)$ كالآتى :

$$.: Map(X,G) \times Map(X,G) \;\to\; Map(X,G)$$
$$(f,g) \;\mapsto\; fg$$

عندئذ فإن $(Map(X,G),.)$ زمرة . لأن :

$$\forall x\in X\ \forall f,g,h\in Map(X,G):$$

$$((fg)h)(x):=(fg)(x)h(x):=(f(x)g(x))h(x) \underset{\text{زمرة } G}{=} f(x)(g(x)h(x))$$

$$=: f(x)gh(x)=:(f(gh))(x)$$

$$\Rightarrow (fg)h=f(gh)$$

نعرف العنصر المحايد $1_{Map(X,G)}$ فى $Map(X,G)$ كالآتى :

(e العنصر المحايد فى G) $\forall x\in X:1_{Map(X,G)}(x)=e$.

$$\forall f\in Map(X,G)\forall x\in X:(1_{Map(X,G)}f)(x)=1_{Map(X,G)}(x)f(x)$$

$$=ef(x)=f(x)\Rightarrow \forall f\in Map(X,G):1_{Map(X,G)}f=f$$

أى أن $1_{Map(X,G)}$ هو العنصر المحايد فى $Map(X,G)$.

والآن ليكن $f\in Map(X,G)$. نظراً لأن G زمرة إذن كل عنصر له معكوس .

إذن

$$\forall x\in X\ \ \exists g\in Map(X,G):(gf)(x):=g(x)f(x)=e=1_{Map(X,G)}(x)$$

$$\Rightarrow\ \ \forall f\in Map(X,G)\exists g\in Map(X,G):gf=1_{Map(X,G)}$$

أى أن لكل $f\in Map(X,G)$ يوجد معكوس $g\in Map(X,G)$.

<u>**١-٢-٦ نظرية**</u> : لتكن $(G,.)$ شبه زمرة . التقريرات الآتية متكافئة :

(١) $(G,.)$ زمرة .

(٢) تناظر أحادى $\forall a\in G\ [G\ni b\overset{a_\ell}{\mapsto} ab\in G$

تناظر أحادى] $G\ni b\overset{a_r}{\mapsto} ba\in G$

(٣) راسم غامر (شامل) $\forall a\in G\ [G\ni b\overset{a_\ell}{\mapsto} ab\in G$

راسم غامر (فوقى)] $G\ni b\overset{a_r}{\mapsto} ba\in G$

<u>**البرهان**</u> : "(٢) $\Leftarrow$ (٣)" : تافه (trivial)

"(١) $\Leftarrow$ (٢)" : الراسم العكسى لـــ a_ℓ هو a_ℓ^{-1} لأن :

$$G\ni b\overset{a_\ell^{-1}}{\mapsto} a^{-1}b\in G$$

$$b \overset{a_\ell}{\longmapsto} ab \overset{a_\ell^{-1}}{\longmapsto} a^{-1}(ab) = (a^{-1}a)b = b$$

1_G

(المقصود بـــ 1_G الراسم G إلى G الذى يرسم كل عنصر فى نفسه)

$$b \overset{a_\ell^{-1}}{\longmapsto} a^{-1}b \overset{a_\ell}{\longmapsto} a(a^{-1}b) = (aa^{-1})b = b$$

1_G

رأينا أن $a_\ell^{-1}a_\ell = 1_G$ ، $a_\ell a_\ell^{-1} = 1_G$ أى أن a_ℓ^{-1} هو بالفعل الراسم العكسى للراسم a_ℓ .
الراسم العكسى لـــ a_r هو a_r^{-1} والبرهان مشابه تماماً لهذا البرهان .

"(٣) ⇐ (١)" : (أ) وجود العنصر المحايد :

ليكن $a \in G$ (هذا ممكن لأن $G \neq \phi$) . لأن a_ℓ راسم غامر(شامل) فإنه يوجد $e \in G$ بحيث يكون $ae = a$.

ليكن $b \in G$. لأن a_r راسم غامر (فوقى) فإنه يوجد $c \in G$ بحيث إن $ca = b$

$$\Rightarrow \quad be = cae = ca = b$$

$$\Rightarrow \quad \forall b \in G \; : \; be = b$$

وبالتماثل يمكن البرهنة على أنه يوجد $e^* \in G$ بحيث يكون :

$$\forall b \in G \; : \; e^*b = b$$

$$\Rightarrow \quad e^* = e^*e = e$$

ويستلزم هذا أن يكون e هو العنصر المحايد

(ب) وجود معكوسات العناصر :

ليكن $a \in G$. الآن يوجد العنصر المحايد $e \in G$.

a_ℓ (فوقى) شامل $\Rightarrow \exists a' \in G : aa' = e$

a_r (فوقى) غامر $\Rightarrow \exists a^* \in G : a^*a = e$

نثبت أن $a' = a^*$ كالآتى :

$$a^* = a^* e = a^* a a' = e a' = a'$$

وبهذا يكون لكل $a \in G$ معكوس هو $a^* \in G$.

١-٢-٧ نتيجة : (جدول الزمر)

لتكن G مجموعة منتهية لها الربط "." $(G = \{a_1, a_2, \dots, a_n\})$

.	a_1	a_2	....	a_n
a_1	$a_1.a_1$	$a_1.a_2$	....	$a_1.a_n$
a_2	$a_2.a_1$	$a_2.a_2$	....	$a_2.a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	$a_n.a_1$	$a_n.a_2$	....	$a_n.a_n$

لتكن $(G,.)$ شبه زمرة .

G زمرة إذا ظهرت وفقط إذا ظهرت كل عناصر G فى كل صف وكل عمود فى جدول الزمر .

البرهان : ظهور كل عناصر G فى كل صف وكل عمود معناه ان a_ℓ ، a_r راسمان غامران (شاملان). ومن النظرية (١-٢-٦) تكون $(G,.)$ زمرة .

(لاحظ أنه لأن G منتهية فظهور كل عنصر من عناصر G فى كل صف وكل عمود يتكافأ مع عدم ظهور أى عنصر فى أى صف أو أى عمود مرتين . لاحظ كذلك أن عدم ظهور أى عنصر مرتين فى أى صف وأى عمود معناه أن a_r ، a_ℓ راسمان واحد لواحد . وهذا صحيح لأن a_r ، a_ℓ تناظران أحاديان) .

٣-١ هومومورفيزمات الزمر Group Homomorphisms

١-٣-١ تعريف : لتكن $(G,.)$ ، $(G',.')$ زمرتين (شبيهتى زمرتين). وليكن $\varphi: G \to G'$.

يسمى φ **هومومورفيزماً** من $(G,.)$ إلى $(G',.')$: $\Leftrightarrow$

$$\forall a,b \in G: \ \varphi(a.b) = \varphi(a).'\varphi(b)$$

(ملحوظة : سنكتب للسهولة فيما بعد –غالباً– : $\varphi(ab) = \varphi(a)\varphi(b)$)

١-٣-٢ ملحوظتان : (أ) لتكن G, G' زمرتين ، وليكن e هو عنصر G المحايد ، e' عنصر G' المحايد . عندئذ فإن :

$\varphi(e)=e'$

$\forall a\in G:\quad \varphi(a^{-1})=\varphi(a)^{-1}$

(ب) لتكن G، G'، G'' زمراً . وليكن $\varphi: G\to G'$ ، $\psi: G'\to G''$ هومومورفيزمي زمر. عندئذ فإن : $\psi o \varphi: G\to G''$ هومومورفيزم زمر .

البرهان : (أ) $\varphi(e)=\varphi(ee)=\varphi(e)\varphi(e)$

$\Rightarrow e'=\varphi(e)^{-1}\varphi(e)=\varphi(e)^{-1}(\varphi(e)\varphi(e))=(\varphi(e)^{-1}\varphi(e))\varphi(e)=e'\varphi(e)=\varphi(e)$

كذلك فإنه لكل $a\in G$:

$e'=\varphi(e)=\varphi(a^{-1}a)=\varphi(a^{-1})\varphi(a)$

$\Rightarrow \varphi(a)^{-1}=e'\varphi(a)^{-1}=(\varphi(a^{-1})\varphi(a))\varphi(a)^{-1}=\varphi(a^{-1})(\varphi(a)\varphi(a)^{-1})=\varphi(a^{-1})e'=\varphi(a^{-1})$

(ب) $\forall a,b\in G:(\psi o \varphi)(a.b):=\psi(\varphi(ab)) \quad = \quad \psi(\varphi(a)\varphi(b))$

φ هومومورفيزم

$= \quad \psi(\varphi(a))\psi(\varphi(b))=:(\psi o\varphi)(a)(\psi o\varphi)(b)$

ψ هومومورفيزم

۱-۳-۳ تعريف : لتكن G', G زمرتين ، $\varphi: G\to G'$ هومومورفيزم زمر . $e'\in G'$ هو العنصر المحايد .

نواة (φ) (Kernel (φ)) تعرف كالآتي

$Ker(\varphi):=\{a\in G:\quad \varphi(a)=e'\}$

صورة (φ) (Image (φ))

$\text{Im}(\varphi):=\{a'\in G':\quad \exists a\in G,\ \varphi(a)=a'\}$

۱-۳-٤ تعريف: ليكن G', G زمرتين $\varphi: G\to G'$ هومومورفيزم زمر. يقال إن φ :

مونومورفيزم (monomorphism) إذا كان φ راسماً واحداً لواحد

إبيمورفيزم (epimorphism) إذا كان φ فوقياً (شاملاً ، غامراً)

أيزومورفيزم (isomorphism) (أو تشاكل) إذا كان φ تناظراً أحادياً

وإذا كان $G'=G$ فإن φ يسمى : **إندومورفيزم** (endomorphism)

وإذا كان $G'=G$ ، φ أيزومورفيزم فيقال إن φ **أوتومورفيزم** (automorphism)

ويقال إن زمرتين G', G متشاكلتان (isomorphic) (أيزومورفيزميتان) إذا وجد $\varphi : G \to G'$ أيزومورفيزم (أو تشاكل) وسنكتب فى هذه الحالة $G \cong G'$.

<u>١-٣-٥ ملحوظتان</u> : ليكن G', G زمرتين ، $\varphi : G \to G'$ هومومورفيزم زمر ، $e \in G$ العنصر المحايد . عندئذ فإن :

(أ) φ مونومورفيزم $\Leftrightarrow$ $Ker(\varphi) = \{e\}$

(ب) φ أيزومورفيزم $\Rightarrow$ φ^{-1} أيزومورفيزم .

<u>البرهان</u> : (أ) " $\Rightarrow$ " :

$$\forall a, b \in G : \quad \varphi(a) = \varphi(b)$$

$$\Rightarrow \varphi(ab^{-1}) \underset{\text{١-٣-٢}}{=} \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = \varphi(b)\varphi(b)^{-1} = e'$$

$$\Rightarrow ab^{-1} \underset{\text{١-٣-٣}}{\in} Ker(\varphi) = \{e\} \Rightarrow ab^{-1} = e$$

$$\Rightarrow a = ae = a(b^{-1}b) = (ab^{-1})b = eb = b \Rightarrow$$ φ واحد لواحد

$\underset{\text{١-٣-٤}}{\Rightarrow}$ φ مونومورفيزم

" $\Leftarrow$ " : من (١-٣-٢) نعلم أن $\varphi(e) = e'$ وهذا يستلزم أن $e \in Ker(\varphi)$ أى أن $\{e\} \subset Ker(\varphi)$ (1) . والآن ليكن $a \in Ker(\varphi)$ هذا يستلزم أن $\varphi(a) = e'$. لكن $\varphi(e) = e'$ (من (١-٣-٢)). وبالتالى فإن $\varphi(a) = \varphi(e)$. ولكن φ مونومورفيزم يعنى أن φ هومومورفيزم واحد لواحد وبالتالى فإن $a = e$ وبالتالى فإن $Ker(\varphi) \subset \{e\}$ (2) . من (1) ، (2) ينتج المطلوب مباشرة .

(ب) نعلم أن φ تناظر أحادى $\Leftarrow$ φ^{-1} معرف وتناظر أحادى

يتبقى أن نبرهن على أن φ^{-1} هومومورفيزم زمر .

ليكن $a', b' \in G'$. لأن φ تناظر أحادى فإنه يوجد واحد بالضبط $a \in G$ بحيث يكون $\varphi(a) = a'$ ، ويوجد واحد بالضبط $b \in G$ بحيث يكون $\varphi(b) = b'$.

والآن :

$$\varphi^{-1}(a'b') = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = (\varphi^{-1}o\varphi)(ab)$$
$$= 1_G(ab) = ab = \varphi^{-1}(a')\varphi^{-1}(b')$$

أى أن φ^{-1} هومومورفيزم .

(المقصود بـــ 1_G هو الراسم : $\begin{matrix} 1_G : G \to G \\ a \mapsto a \end{matrix}$ يسمى راسم الوحدة على G)

١-٣-٦ ملحوظة : لتكن $G_i(i=1,2,3,4)$ زمراً وليكن كل من :

$f : G_1 \to G_2$ ، $g : G_2 \to G_3$ ، $h : G_3 \to G_4$ هومومورفيزماً . عندئذ فإن :

(أ) $\begin{matrix} 1_{G_i} : G_i \to G_i \\ a \mapsto a \end{matrix}$ أيزومومورفيزم

(ب) $(hog)of = ho(gof)$

(جـ) $1_{G_2}of = f$ ، $go1_{G_2} = g$

البرهان : (أ) نعلم أن 1_{G_i} تناظر أحادى . والآن :

$$\forall a,b \in G_i : 1_{G_i}(ab) = ab = 1_{G_i}(a)1_{G_i}(b)$$

(ب) هذا صحيح لجميع الرواسم ومن ثم فإنه صحيح لجميع الهومومورفيزمات (لاحظ أن $(hog)of$ هومومورفيزم من (١-٣-٢)) .

(جـ) $\forall a \in G_1 : (1_{G_2}of)(a) = 1_{G_2}(f(a)) = f(a) \Rightarrow 1_{G_2}of = f$

$$\forall a \in G_2 : (go1_{G_2})(a) = g(1_{G_2}(a)) = g(a) \Rightarrow go1_{G_2} = g$$

(لاحظ تساوى النطاقات والنطاقات المصاحبة)

١-٣-٧ تعريف : لتكن G زمرة . الراسم

$$\forall a \in G : \varphi_a : G \to G$$
$$x \mapsto axa^{-1}$$

أوتومورفيزم . هذا واضح لأن له راسماً عكسياً هو

$$\varphi_{a^{-1}} : G \to G$$
$$x \mapsto a^{-1}xa$$

$$\forall x \in G : (\varphi_{a^{-1}}o\varphi_a)(x) = \varphi_{a^{-1}}(\varphi_a(x)) = \varphi_{a^{-1}}(axa^{-1}) = a^{-1}(axa^{-1})a$$
$$= (a^{-1}a)x(a^{-1}a) = x ,$$

$$\Rightarrow \quad \varphi_{a^{-1}} o \varphi_a = 1_G \qquad (1)$$

$$(\varphi_a o \varphi_{a^{-1}})(x) = \varphi_a(\varphi_{a^{-1}}(x)) = \varphi_a(a^{-1}xa) = a(a^{-1}xa)a^{-1}$$
$$= (aa^{-1})x\,(aa^{-1}) = x$$

$$\Rightarrow \quad \varphi_a o \varphi_{a^{-1}} = 1_G \qquad (2)$$

من (1) ، (2) ينتج أن φ تناظر أحادى . والآن

$$\forall x, y \in G : \varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$$

أى أن φ_a هومومورفيزم وهو كذلك تناظر أحادى من G إلى G إذن هو أوتومورفيزم على G .

والآن أى أوتومورفيزم φ على G يسمى <u>أوتومورفيزم داخلى</u>(inner automorphism) لـــ G إذا وجد $a \in G$ بحيث يكون $\varphi_a = \varphi$.

<u>١-٣-٨ أمثلة</u> :

<u>مثال ١</u> : لأى $m \in \mathbb{Z}$ الراسم :

$$\varphi_m : \mathbb{Z} \to \mathbb{Z}$$
$$n \mapsto mn$$

هومومورفيزم لأنَ :

$$\forall n, p \in \mathbb{Z} : \varphi_m(n+p) = m(n+p) = mn + mp = \varphi_m(n) + \varphi_m(p)$$

وبالتالى فهو إندومورفيزم

ولأى $m \neq 0$ يكون كذلك مونومورفيزم لأن :

$$\forall p, q \in \mathbb{Z} : \varphi_m(p) = \varphi_m(q) \Rightarrow mp = mq \Rightarrow p = q$$

<u>مثال ٢</u> : الراسم الأ سى :

$$e^{-} : (\mathbb{R}, +) \to (\mathbb{R}^*_+, .)$$
$$x \mapsto e^x$$

أيزومورفيزم لأن :

$$\forall x, y \in \mathbb{R} : e^{-}(x+y) = e^{x+y} = e^x e^y = e^{-}(x)e^{-}(y)$$

ولإثبات أنه تناظر أحادى (وبالتالى يكون أيزومورفيزم) يكفى أن نعطى الراسم العكسى وهو :

$$Log_e - : (\mathbb{R}_+^*, .) \to (\mathbb{R}, +)$$
$$x \mapsto Log_e x$$

والآن

$$e^{Log_e -} : (\mathbb{R}_+^*, .) \to (\mathbb{R}_+^*, +)$$
$$x \mapsto e^{Log_e x} = x$$

أى أن

$$e^{Log_e -} = 1_{\mathbb{R}_+^*} \qquad (1)$$

كذلك فإن :

$$Log_e e^- : (\mathbb{R}, +) \to (\mathbb{R}, +)$$
$$x \mapsto Log_e e^x = xLog_e e = x$$

أى أن

$$Log_e e^- = 1_{\mathbb{R}} \qquad (2)$$

من (1) ، (2) يتضح أن الراسم $Log_e - : \mathbb{R}_+^* \to \mathbb{R}$ هو الراسم العكسى للراسم $e^- : \mathbb{R} \to \mathbb{R}_+^*$ ، وبالتالى فإن كلا منهما يكون تناظراً أحادياً ، ومن ثم البرهان .

<u>مثال ٣</u> : لتكن G زمرة ، e عنصرها المحايد .

(أ) النقل الأيسر ℓ_a هومومورفيزم $\Leftrightarrow a = e$

النقل الأيمن r_a هومومورفيزم $\Leftrightarrow a = e$

(ب) الراسم : $\varphi : G \to \gamma(G)$ ، $a \mapsto \ell_a$ هومومورفيزم

(جـ) : $\psi : G \to \gamma(G)$ ، $a \mapsto r_a$ هومومورفيزم

إذا كانت وفقط إذا كانت G إبدالية

<u>البرهان</u> : (أ) ليكن $\ell_a : G \to G$ ، $x \mapsto ax$ هومومورفيزم $\Leftarrow$

$$\forall x, y \in G : axy = \ell_a(xy) = \ell_a(x)\ell_a(y) = axay$$
$$\Rightarrow a = e$$

وبالعكس

$$a = e \Rightarrow \ell_a(xy) = \ell_e(xy) = exy = exey = \ell_e(x)\ell_e(y) = \ell_a(x)\ell_a(y)$$

أى أن $\ell_a = \ell_e$ هومومورفيزم

(ب) ليكن $a,b \in G$ المطلوب إثبات أن $\varphi(ab) = \varphi(a)\varphi(b)$ ، أى المطلوب إثبات أن $\ell_{ab} = \ell_a \ell_b$ والآن

$$\forall x \in G : \ell_{ab}(x) = (ab)x = a(bx) = \ell_a(\ell_b(x)) = (\ell_a \ell_b)(x)$$

$$\Rightarrow \ell_{ab} = \ell_a \ell_b$$

(جـ) " $\Rightarrow$ " :

$$\psi \text{ هومومورفيزم } \Rightarrow \forall a,b \in G : \psi(ab) = \psi(a)\psi(b)$$

أى أن

$$\forall a,b \in G : r_{ab} = r_a r_b$$

$$\Rightarrow \forall a,b,x \in G : r_{ab}(x) = (r_a r_b)(x) = r_a(r_b(x)) = r_a(xb) = (xb)a = x(ba)$$

أيضا $r_{ab}(x) = x(ab)$. بأخذ $x = e$ (العنصر المحايد فى G) ينتج أن $\forall a,b \in G : ab = ba$.

أى أن G إبدالية .

" $\Leftarrow$ " : لتكن G إبدالية هذا يقتضى أن :

$$\forall a,b \in G : ab = ba \Rightarrow \forall a,b,x \in G : xab = xba$$

$$\Rightarrow \forall a,b,x \in G : r_{ab}(x) = x(ab) = x(ba) = (xb)a = r_a(xb) = r_a(r_b(x)) = (r_a r_b)(x)$$

$$\Rightarrow r_{ab} = r_a r_b \Rightarrow \psi(ab) = \psi(a)\psi(b) \Rightarrow \psi \text{ هومومورفيزم}$$

المقصود بـ $\ell_a \ell_b$ هو $\ell_a o \ell_b$ ، وكذلك $r_a r_b$ تعنى $r_a o r_b$ حيث "o" هى العملية فى الزمرة $\gamma(G)$.

__مثال ٤__ : برهن على أن $f : \mathbb{C} \to \mathbb{R}$

$$x + iy \mapsto x$$

هومومورفيزم من $(\mathbb{C},+)$ إلى $(\mathbb{R},+)$. اوجد نواة (f) هل f شامل (غامر) ؟

__الحـل__ :

$$\forall x_1 + iy_1, x_2 + iy_2 \in \mathbb{C} : f(x_1 + iy_1 + x_2 + iy_2) = f(x_1 + x_2 + i(y_1 + y_2)) = x_1 + x_2$$
$$= f(x_1 + iy_1) + f(x_1 + iy_2)$$

هومومورفيزم $\Rightarrow f$

$$Ker(f)=\{x+iy\in\mathbb{C}:f(x+iy)=x=0\}$$
$$=\{iy \mid y\in\mathbb{R}\}$$

واضح أن f شامل (غامر)

مثال ٥ : برهن على أن $f:\mathbb{C}\setminus\{0\}\rightarrow\mathbb{R}\setminus\{0\}$

$$z\mapsto |z|$$

هومومورفيزم من $(\mathbb{C}\setminus\{0\},.)$ إلى $(\mathbb{R}\setminus\{0\},.)$ واوجد نواته

الحـــل :

$$\forall z_1,z_2\in\mathbb{C}\setminus\{0\}:f(z_1z_2)=|z_1z_2|=|z_1||z_2|=f(z_1)f(z_2)$$

هومومورفيزم $\Rightarrow f$

$$Ker(f)=\{z\in\mathbb{C}\setminus\{0\}:f(z)=1\}$$
$$=\{z\in\mathbb{C}\setminus\{0\}:|z|=1\}$$

دائرة فى مستوى z مركزها (o,o) ونصف قطرها 1 .

مثال ٦ : برهن على أن : $f:\mathbb{C}\rightarrow\mathbb{C}\setminus\{0\}$

$$z\mapsto e^z$$

هو إبيمورفيزم من $(\mathbb{C},+)$ إلى $(\mathbb{C}\setminus\{0\},.)$ واوجد نواته .

الحـــل :

$$\forall z_1,z_2\in\mathbb{C}:f(z_1+z_2)=e^{z_1z_2}=e^{z_1}e^{z_2}=f(z_1)f(z_2)\Rightarrow f$$ هومومورفيزم

$$Ker(f)=\{z\in\mathbb{C}\mid f(z)=e^z=1\}$$
$$=\{z\in\mathbb{C}\mid e^x(\cos y+i\sin y)=1\}$$
$$=\{z\in\mathbb{C}\mid e^x\cos y=1, e^x\sin y=0\}$$

$$e^x\sin y=0\Rightarrow\sin y=0\Rightarrow y=n\pi, n\in\mathbb{Z}$$
$$e^x\cos y=1\Rightarrow\cos y\geq 0\underset{y=n\pi}{\Rightarrow} y=2k\pi, k\in\mathbb{Z}\Rightarrow e^x=1\Rightarrow x=0$$
$$\Rightarrow z=2ik\pi$$

أى أن

$$Ker(f)=\{z\in\mathbb{C}\mid z=2ik\pi, k\in\mathbb{Z}\}$$

لأى $w\in\mathbb{C}\setminus\{0\}$ يوجد $Log_e w\in\mathbb{C}$ بحيث إن $f(Log_e w)=e^{Log_e w}=w$ وبالتالى يكون f راسماً غامراً (فوقياً)

مثال ٧ : برهن على ان الراسم $\begin{array}{c}\varphi:\mathbb{C}\setminus\{0\}\to\mathbb{C}\setminus\{0\}\\ x\mapsto x^4\end{array}$ هومومورفيزم . اوجد نواته

الحــل :

هومومورفيزم $\forall x,y\in\mathbb{C}\setminus\{0\}:\varphi(xy)=(xy)^4=x^4y^4=\varphi(x)\varphi(y)\Rightarrow\varphi$

$$\begin{aligned}Ker(\varphi)&=\{x\mid x\in\mathbb{C}\setminus\{0\},\varphi(x)=1\}\\&=\{x\in\mathbb{C}\setminus\{0\},x^4=1\}\end{aligned}$$

$$x^4=1=\cos 0+i\sin 0\Rightarrow x=\cos\frac{0+2k\pi}{4}+i\sin\frac{0+2k\pi}{4},k=0,1,2,3$$

(نظرية دى موافر)

$$k=0\Rightarrow x=\cos 0+i\sin 0=1$$
$$k=1\Rightarrow x=\cos\frac{2\pi}{4}+i\sin\frac{2\pi}{4}=i$$
$$k=2\Rightarrow x=\cos\pi+i\sin\pi=-1$$
$$k=3\Rightarrow x=\cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2}=-i$$

أى أن $Ker(\varphi)=\{1,i,-1,-i\}$

مثال ٨ : برهن او انف : $\begin{array}{c}f:\mathbb{R}\to\mathbb{Z}\\ x\mapsto\lfloor x\rfloor\end{array}$ هومومورفيزم من $(\mathbb{R},+)$ إلى $(\mathbb{Z},+)$

($\lfloor x\rfloor$: اكبر عدد صحيح $\le x$ يسمى floor x)

الحــل : f ليس هومومورفيزماً . مثال مضاد :

$$f\left(\frac{1}{2}+\frac{1}{2}\right)=f(1)=\lfloor 1\rfloor=1$$

بينما

$$f\left(\frac{1}{2}\right)+f\left(\frac{1}{2}\right)=\left\lfloor\frac{1}{2}\right\rfloor+\left\lfloor\frac{1}{2}\right\rfloor=0+0=0$$

مثال ٩ : برهن أو انف : لايمكن أن يوجد أيزومورفيزم (تشاكل) بين زمرتين إحداهما إبدالية والأخرى غير إبدالية .

البرهان : ليكن لدينا زمرتان G إبدالية ، H غير إبدالية ، وليكن $\varphi : G \to H$ أيزومورفيزم. لأن H غير إبدالية فإنه يوجد $a', b' \in H$ بحيث إن $a'b' \neq b'a'$. ولأن φ أيزوموموروفيزم إذن يوجد واحد بالضبط a ، وواحد بالضبط b بحيث يكون $\varphi(b) = b', \varphi(a) = a'$.

والآن

$$a'b' = \varphi(a)\varphi(b) \underset{\text{هومومورفيزم } \varphi}{=} \varphi(ab) \underset{\text{إبدالية } G}{=} \varphi(ba) \underset{\text{هومومورفيزم } \varphi}{=} \varphi(b)\varphi(a)$$

تناقض $= b'a'$

طريقة أخرى : نفترض هذه المرة أن G غير إبدالية ، H إبدالية . G غير إبدالية إذن يوجد $a,b \in G$ بحيث يكون $ab \neq ba$. ولأن φ أيزوموموروفيزم فإن $\varphi(ab) \neq \varphi(ba)$

ولكن :

$$\varphi(ab) \underset{\text{هومومورفيزم } \varphi}{=} \varphi(a)\varphi(b) \underset{\text{إبدالية } H}{=} \varphi(b)\varphi(a) \underset{\text{هومومورفيزم } \varphi}{=} \varphi(ba)$$: تناقض

مثال ١٠ : برهن على أنه لايمكن أن يوجد إبيمورفيزم من $(\mathbb{Q},+)$ على $(\mathbb{Z},+)$

البرهان : ليكن $\varphi : (\mathbb{Q},+) \to (\mathbb{Z},+)$ إبيمورفيزم . إذن يوجد $x \in \mathbb{Q}$ بحيث يكون $\varphi(x) = 1$. والآن

$$1 = \varphi(x) \underset{x \in \mathbb{Q}}{=} \varphi\left(\frac{x}{2} + \frac{x}{2}\right) \underset{\text{هومومورفيزم } \varphi}{=} \varphi\left(\frac{x}{2}\right) + \varphi\left(\frac{x}{2}\right) = 2\varphi\left(\frac{x}{2}\right)$$

تناقض $\Rightarrow \varphi\left(\frac{x}{2}\right) = \frac{1}{2} \notin (\mathbb{Z},+)$

مثال ١١: برهن على أنه لايمكن أن يوجد إبيمورفيزم من $(\mathbb{Q},+)$ على $(\mathbb{Q}\setminus\{0\},.)$

البرهان : ليكن $\varphi : (\mathbb{Q},+) \to (\mathbb{Q}\setminus\{0\},.)$ إبيمورفيزم .

لآن φ شامل (غامر) فإنه يوجد $x \in \mathbb{Q}$ بحيث ان $\varphi(x) = 3$. والآن

$$3 = \varphi(x) = \varphi\left(\frac{x}{2} + \frac{x}{2}\right) \underset{\text{هومومورفيزم } \varphi}{=} \varphi\left(\frac{x}{2}\right)\varphi\left(\frac{x}{2}\right) \Rightarrow \varphi\left(\frac{x}{2}\right) = \sqrt{3} \notin \mathbb{Q}\setminus\{0\}$$:تناقض

١-٤ الزمر الجزئية Subgroups

١-٤-١ تعريف : لتكن G زمرة . ولتكن H مجموعة جزئية (غير خالية) من G .
يقال إن H **زمرة جزئية** (Subgroup) من G إذا تحقق :
(أ) لكل $a,b\in H$: $ab\in H$.
(ب) المجموعة H مع الربط المستحدث $\begin{matrix} H\times H\to H \\ (a,b)\mapsto ab \end{matrix}$ تكون زمرة

يلاحظ ان كل زمرة G تحتوى على زمرتين جزئيتين (تافهتين) هما G نفسها ، $\{e\}$ حيث e عنصرها المحايد.

١-٤-٢ تمهيدية : لتكن G زمرة . H مجموعة جزئية (غير خالية) من G .
H زمرة جزئية من G إذا كان وفقط إذا كان لكل عنصرين $a,b\in H$: $ab^{-1}\in H$.

البرهان : " $\Leftarrow$ "H : زمرة جزئية ، $ab^{-1}\in H \Leftarrow a,b^{-1}\in H \Leftarrow a,b\in H$

" $\Rightarrow$ "H : غير خالية $\Leftarrow$ يوجد عنصر $e=bb^{-1}\in H \Leftarrow b\in H$

والآن لكل $b\in H$: $b^{-1}=eb^{-1}\in H$ (لأن $e\in H$)

ولكل $ab=a(b^{-1})^{-1}\in H \Leftarrow a,b^{-1}\in H : a,b\in H$

١-٤-٣ : ملحوظة : ليكن $\varphi: G\to G'$ هومومورفيزم زمر . عندئذ فإن
(أ) H زمرة جزئية من G $\Leftarrow \varphi(H)$ زمرة جزئية من G' . وعلى وجه الخصوص فإن صورة (φ) $(\mathrm{Im}(\varphi))$ زمرة جزئية من G' .
(ب) H' زمرة جزئية من G' $\Leftarrow$ $\varphi^{-1}(H'):=\{a\in G:\varphi(a)\in H'\}$ زمرة جزئية من G . وعلى وجه الخصوص فإن نواة (φ) $(Ker(\varphi))$ زمرة جزئية من G .

البرهان : (أ) $e\in H\Rightarrow \varphi(e)\in\varphi(H)$

أى أن $\varphi(H)$ غير خالية .

والآن : $a',b'\in\varphi(H)\Rightarrow \exists\, a,b\in H : a'=\varphi(a), b'=\varphi(b)$

$$\Rightarrow a'(b')^{-1}=\varphi(a)\varphi(b)^{-1} \underset{\text{١-٣-٢ (أ)}}{=} \varphi(a)\varphi(b^{-1})=\varphi(ab^{-1})\in\varphi(H)$$

$\Rightarrow \quad G'$ زمرة جزئية من $\varphi(H)$

١-٤-٢

والآن : زمرة جزئية $\operatorname{Im}(\varphi) = \varphi(G) \subset G' \Rightarrow$ زمرة $G \subset G$

(ب) ليكن e' هو عنصر G' المحايد ، e هو عنصر G المحايد . e' عنصر فى H' لأن H' زمرة جزئية من G' .

$$\varphi(e) \quad = \quad e' \in H' \Rightarrow e \in \varphi^{-1}(H')$$

١-٣-٢ (أ)

أى أن $\varphi^{-1}(H')$ مجموعة غير خالية

والآن :

$$a,b \in \varphi^{-1}(H') \Rightarrow \varphi(a),\varphi(b) \in H' \Rightarrow \varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1})$$

$= \quad \varphi(a)\varphi(b)^{-1} \in H' \Rightarrow ab^{-1} \in \varphi^{-1}(H') \quad \Rightarrow \quad G$ زمرة جزئية من $\varphi^{-1}(H')$

١-٣-٢ (أ)   ١-٤-٢

ولأن $\{e'\}$ زمرة جزئية (تافهة) من G' فإن : $Ker(\varphi) = \varphi^{-1}(\{e'\})$ زمرة جزئية من G .

١-٤-٤ أمثلة :

مثال ١: (أ) المجموعة $Aut(G)$ مجموعة الأوتومورفيزمات على G حيث G زمرة تكون زمرة جزئية من الزمرة $(\gamma(G),o)$ (انظر مثال (١-٢-٥)) .

(ب) الراسم

$$\varphi : G \to Aut(G)$$
$$a \mapsto \varphi_a$$

هومومورفيزم زمر .

(جـ) المجموعة $Int(G)$ مجموعة جميع الأوتومورفيزمات الداخلية زمرة جزئية من الزمرة $Aut(G)$ وبالتالى فهى زمرة جزئية من $\gamma(G)$.

البرهان : (أ) واضح أن $\begin{matrix} 1_G : G \to G \\ a \mapsto a \end{matrix}$ أوتومورفيزم وبالتالى فإن $Aut(G)$ مجموعة ليست خالية.

$$\varphi,\psi \in Aut(G) \;\Rightarrow\; \varphi,\psi^{-1} \in Aut(G) \;\Rightarrow\; \varphi o \psi^{-1} \in Aut(G) \;\Rightarrow\; Aut(G)$$

١-٣-٥   ١-٣-٢ (ب)   ١-٤-٢

زمرة جزئية من $(\gamma(G),o)$.

ب) $\forall a,b,x \in G : \varphi(ab)(x) = \varphi_{ab}(x) = abx(ab)^{-1} = a(bxb^{-1})a^{-1}$

$$= \varphi_a(bxb^{-1}) = (\varphi_a o \varphi_b)(x) = (\varphi(a) o \varphi(b))(x)$$

$$\Rightarrow \forall a,b \in G \quad \varphi(ab) = \varphi(a) o \varphi(b)$$

$\Rightarrow \quad \varphi$ هومومورفيزم

جـ) $1_G : G \to G$

$$x \mapsto x = exe^{-1}$$

$$\Rightarrow \quad 1_G \in Int(G)$$

نعرف $\varphi_a^{-1} \in Int(G)$ كالآتى :

$$\forall x \in G : \varphi_a^{-1}(x) := a^{-1}xa. \ (\varphi_a^{-1} o \varphi_a)(a) = a^{-1}axa^{-1}a = x \Rightarrow \varphi_a^{-1} o \varphi_a = 1_G$$

$$(\varphi_a o \varphi_a^{-1})(x) = aa^{-1}xaa^{-1} = x \Rightarrow \varphi_a o \varphi_a^{-1} = 1_G$$

أى أن φ_a^{-1} هو معكوس φ_a . والآن :

$$\forall \varphi_a, \varphi_b \in Int(G) \ \forall x \in G : (\varphi_a o \varphi_b^{-1})(x) = ab^{-1}xba^{-1} = ab^{-1}x(ab^{-1})^{-1}$$

$= \varphi_{ab^{-1}}(x) \Rightarrow \varphi_a o \varphi_b^{-1} \in Int(G) \Rightarrow Aut(G)$ زمرة جزئية من $Int(G)$

مثال ٢ :

ليكن $\pi := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ ، $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ عنصرين فى γ_4 عندئذ فإن :

$H := \{1_{\gamma_4}, \pi, \sigma, \pi \circ \sigma\}$ زمرة جزئية (ذات أربعة عناصر) من γ_4 وهى إبدالية ، ويتحقق لها :

$\pi o \pi = \sigma o \sigma = (\pi o \sigma) o (\pi o \sigma) = 1_{\gamma_4}$ (العنصر المحايد فى γ_4 = 1_{γ_4})

البرهان :

$$\pi o \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\sigma o \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \pi o \sigma$$

$$\pi o \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = 1_{\gamma_4}$$

$$\sigma o \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = 1_{\gamma_4}$$

$$(\pi o \sigma) o (\pi o \sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = 1_{\gamma_4}$$

$$(\pi o \sigma) o \sigma = \pi \quad , \quad (\pi o \sigma) o \pi = (\sigma o \pi) o \pi = \sigma$$

$$\sigma o (\pi o \sigma) = \sigma o (\sigma o \pi) = \pi \quad , \quad \pi o (\pi o \sigma) = \sigma$$

(كل زمرة ذات أربعة عناصر $H = \{a,b,c,e\}$ ، يتحقق لها : $a^2 = b^2 = c^2 = e$

تسمى **زمرة كلاين الرباعية** (Klein 4-group)

مثال ٣ : H زمرة جزئية من $(\mathbb{Z},+)$ إذا كان وفقط إذا كان يوجد $m \in \mathbb{Z}$ بحيث أن $H = m\mathbb{Z} := \{mk : k \in \mathbb{Z}\}$.

البرهان : "$\Rightarrow$" : لأى $m \in \mathbb{Z}$ الراسم

$$\mu_m : \mathbb{Z} \to \mathbb{Z}$$
$$k \mapsto mk$$

إندومورفيزم لـــ $(\mathbb{Z},+)$ (انظر (١-٣-٨) مثال ١) . ومن ثم فإن $m\mathbb{Z} = \mu_m(\mathbb{Z})$ زمرة جزئية من $\mathbb{Z}$ (انظر (١-٤-٣) (أ))

طريقة أخرى : $0 = m.0 \in m\mathbb{Z} \Rightarrow m\mathbb{Z} \neq \phi$

$\forall mk, m\ell \in m\mathbb{Z}: \ mk - m\ell = m(k-\ell) \in m\mathbb{Z} \ \Rightarrow$ $m\mathbb{Z}$ زمرة جزئية من $\mathbb{Z}$

١-٤-٢

"$\Leftarrow$" : لتكن H زمرة جزئية من $(\mathbb{Z},+)$. إذا كانت $H = \{0\}$ ، خذ $m = 0$. إذا كانت $H \neq \{0\}$ ، فلاحظ أن $k \in H \Leftarrow -k \in H$ وبهذا تحتوى H أيضاً على أعداد صحيحة موجبة. وليكن m هو أصغر عدد صحيح موجب فى H . نثبت أن $H = m\mathbb{Z}$.

"$\supset$" : $H \subset \mathbb{Z}$ زمرة جزئية ، $m \in H \ \Leftarrow \ m\mathbb{Z} \subset H$ (1)

"$\subset$" : ليكن $x \in H$. عندئذ فإنه يوجد $k, r \in \mathbb{Z}$ بحيث $0 \le r < m$ ، $x = km + r$.

ولأن H زمرة جزئية من $\mathbb{Z}$ فإنه ينتج أن $r = x - km \in H$

ولأن m هو أصغر عدد صحيح موجب فى H، r عنصر فى H يحقق $0 \leq r < m$
فإنه ينتــج أن $r = 0$. وبالتالى فإن $x = km \in m\mathbb{Z}$ ، أى أن $H \subset m\mathbb{Z}$ (2)
من (1) ، (2) ينتج أن $H = m\mathbb{Z}$.

مثال ٤ : ليكن $i := \sqrt{-1} \in \mathbb{C}$ ، وليكن

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

المجموعة $Q := \{E, -E_1, I, -I_1, J, -J, K, -K\}$ زمرة جزئية غير إبدالية من الزمرة $GL(2,\mathbb{C})$ زمرة جميع المصفوفات من النوع 2×2 القابلة للعكس وعناصرها (مداخلها) أعداد مركبة تسمة هذه الزمرة **الزمرة الرباعية** (The quaternion group)

يستطيع القارئ أن يتحقق بسهولة من جدول "الضرب" الآتى :

.	E	I	J	K
E	E	I	J	K
I	I	$-E$	K	$-J$
J	J	$-K$	$-E$	I
K	K	J	$-I$	$-E$

مثال ٥ : برهن أو انف :

(أ) $(\mathbb{Z},+)$ زمرة جزئية من $(\mathbb{Q},+)$
(ب) $(\mathbb{N},+)$ زمرة جزئية من $(\mathbb{Q},+)$
(جـ) $(\mathbb{Q},+)$ زمرة جزئية من $(\mathbb{C},+)$
(د) $(\mathbb{Z},+)$ زمرة جزئية من $(\mathbb{Q}\setminus\{0\},.)$
(هـ) $(\mathbb{Q}\setminus\{0\},.)$ زمرة جزئية من $(\mathbb{C}\setminus\{0\},.)$
(و) $(\mathbb{Q}\setminus\{0\},.)$زمرة جزئية من زمرة الأعداد الحقيقية التى لها الشكل $a+b\sqrt{2}$ حيث
$a,b \in \mathbb{Q}$, $a + b\sqrt{2} \neq 0$

الحــل : (أ) $0\in\mathbb{Z}$ أى أن $\mathbb{Z}\neq\phi$ ، $\mathbb{Z}\subset\mathbb{Q}$ ($\mathbb{Z}$ مجموعة جزئية من $\mathbb{Q}$)

$\forall a,b\in\mathbb{Z}: a-b\in\mathbb{Z} \Rightarrow$ $(\mathbb{Z},+)$ زمرة جزئية من $(\mathbb{Q},+)$

(ب) $1\in\mathbb{N}\subset\mathbb{Q}$ ومعكوس 1 بالنسبه للعملية + هو -1 . لكن $-1\notin\mathbb{N}$ وبالتالى فإن $(\mathbb{N},+)$ ليست زمرة جزئية من $(\mathbb{Q},+)$.

(جـ) $0\in\mathbb{Q}\in\mathbb{C}$ ، أى أن $\mathbb{Q}\neq\phi$ ، وهى مجموعة جزئية من $\mathbb{C}$ ، (أى عنصر $p\in\mathbb{Q}$ يمكن أن يكتب على الصورة $p+0i$ وبالتالى يكون عنصراً فى $\mathbb{C}$.)

$(\mathbb{Q},+)$ زمرة جزئية من $(\mathbb{C},+)$ $\Rightarrow$ $\forall a,b\in\mathbb{Q}: a-b\in\mathbb{Q}$.

(د) $(\mathbb{Z},+)$ ليست زمرة جزئية من $(\mathbb{Q}\setminus\{0\},.)$ لأن العملية "+" على $\mathbb{Z}$ "تختلف" عن العملية "." على $\mathbb{Q}$.

لاحظ كذلك أن $(\mathbb{Z}\setminus\{0\},.)$ ليست زمرة على الإطلاق لأن معكوس 2 بالنسبه للعملية "." هو $\frac{1}{2}$. $2\in\mathbb{Z}$ لكن $\frac{1}{2}\notin\mathbb{Z}$. وبالتالى فإن $(\mathbb{Z}\setminus\{0\},.)$ لايمكن كذلك أن تكون زمرة جزئية من $(\mathbb{Q}\setminus\{0\},.)$ لأنها ليست زمرة من البداية .

(هـ) $1\in\mathbb{Q}\setminus\{0\}\subset\mathbb{C}\setminus\{0\}$ ، أى أن $\mathbb{Q}\setminus\{0\}$ ليست خالية وهى مجموعة جزئية – كما سبق – من $\mathbb{C}\setminus\{0\}$.

$$\forall a,b\in\mathbb{Q}\setminus\{0\}: ab^{-1}\in\mathbb{Q}\setminus\{0\}$$

وبالتالى فهى زمرة جزئية من $\mathbb{C}\setminus\{0\}$.

(و) $\phi\neq\mathbb{Q}\setminus\{0\}$ كذلك فإن : $\forall a\in\mathbb{Q}\setminus\{0\}: a=a+0\sqrt{2}$

أى أن $\mathbb{Q}\setminus\{0\}\subset\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}, a+b\sqrt{2}\neq 0\}$

$$\forall a,b\in\mathbb{Q}\setminus\{0\}: ab^{-1}\in\mathbb{Q}\setminus\{0\}$$

وبالتالى تكون $(\mathbb{Q}\setminus\{0\},.)$ زمرة جزئية من الزمرة $(\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}, a+b\sqrt{2}\neq 0\},.)$

(على القارئ ان يتحقق من أن مجموعة الأعداد التى على الشكل $a+b\sqrt{2}$ حيث $a,b\in\mathbb{Q}$ وبحيث $a+b\sqrt{2}\neq 0$ تكون زمرة تحت عملية الضرب العادية للأعداد الحقيقية)

مثال ٦ : برهن أو انف :

(أ) تقاطع أى زمرتين جزئيتين من زمرة G هو زمرة جزئية من G .

(ب) اتحاد أى زمرتين جزئيتين من زمرة G هو زمرة جزئية من G .

<u>الحـل</u> : (أ) تقرير صحيح . البرهان :

ليكن H، K زمرتين جزئيتين من G وليكن $e\in G$ عنصرها المحايد . ينتج أن $e\in H$ ، $e\in K$ وبالتالى فإن $e\in H\cap K$ ويكون $H\cap K\neq\phi$. والآن ليكن $a,b\in H\cap K \Leftarrow a,b\in H$ ، $a,b\in K \Leftarrow a,b^{-1}\in H$ ، $ab^{-1}\in K \Leftarrow ab^{-1}\in H\cap K$.

(ب) تقرير خاطئ . مثال مضاد :

$2\mathbb{Z}$ ، $3\mathbb{Z}$ زمرتان جزئيتان من $\mathbb{Z}$ (بصفة عامة كما رأينا فى مثال ٣ $m\mathbb{Z}$ زمرة جزئية من $\mathbb{Z}$ حيث $m\in\mathbb{Z}$) .

والآن $3\in 3\mathbb{Z}$ ، $2\in 2\mathbb{Z}$ لكن : $\quad 1=3-2\notin 2\mathbb{Z}\cup 3\mathbb{Z}$

<u>مثال ٧</u> : لتكن H, K زمرتين جزئيتين من زمرة G . برهن على أن اتحاد H، K زمرة جزئية من G إذا كانت وفقط إذا كانت إحدى الزمرتين زمرة جزئية من الأخرى .

<u>البرهان</u> : برموز واضحة نكتب

$$H\cup K \hookrightarrow G \Leftrightarrow H\hookrightarrow K \vee K\hookrightarrow H$$

($H\hookrightarrow G$ تعنى H زمرة جزئية من الزمرة G)

" $\Leftarrow$ " : واضح

" $\Rightarrow$ " : ليكن $a,b\in H\cup K$ بحيث إن $a\in H$ ، $a\notin K$ ، $b\in K$ ، $b\notin H$.

ينتج أن $ab^{-1}\in H\cup K$ (لأن $H\cup K\hookrightarrow G$). ومن ثم فإن $ab^{-1}\in H$ أو $ab^{-1}\in K$

تناقض $\quad ab^{-1}\in H \Rightarrow ba^{-1}=(ab^{-1})^{-1}\in H \underset{a\in H}{\Rightarrow} b=ba^{-1}a\in H$

نهاية البرهان. تناقض $\quad ab^{-1}\in K \underset{b\in K}{\Rightarrow} a=ab^{-1}b\in K$

<u>مثال ٨</u> : لتكن G زمرة ولتكن $Z:=\{g\in G: gx=xg\ \forall x\in G\}$

برهن على أن Z زمرة جزئية إبدالية من G .

(تسمى <u>مركز Z</u> (Centre or Central of G))

<u>البرهان</u> : $e\in Z$ لأن

$$\forall x\in G: ex=x=xe \qquad (1)$$

$$g\in Z \Rightarrow \forall x\in G: gx=xg \Rightarrow \forall x\in G: x^{-1}g^{-1}=(gx)^{-1}=(xg)^{-1}=g^{-1}x^{-1}$$

$$\Rightarrow \forall y\in G: yg^{-1}=g^{-1}y \Rightarrow g^{-1}\in Z \qquad (2)$$

$$g,h\in Z\Rightarrow \forall x\in G: hgx \underset{g\in Z}{=} hxg \underset{h\in Z}{=} xhg \Rightarrow hg\in Z \qquad (3)$$

من (1) ، (2) ، (3) Z زمرة جزئية من G. ومن التعريف يتضح مباشرة أن Z إبدالية .

مثال ٩ : لتكن G زمرة إبدالية لها العنصر المحايد e . وليكن $n\in\mathbb{N}$. برهن على أن H مجموعة كل العناصر فى G التى تحقق $x^n = e$ تكون زمرة جزئية من G .

البرهــان : $e\in H$ لأن $e^n = e$. ليكن $y\in H \Rightarrow y^n = e \Rightarrow$

$(y^{-1})^n = (y^n)^{-1} = e^{-1} = e$ ، أى أن $y^{-1}\in H$ وكذلك فإن :

$$x,y\in H \Rightarrow x^n = e, y^n = e \Rightarrow (xy)^n = \underbrace{(xy).(xy)...(xy)}_{n \text{ من المرات}} \underset{G \text{ إبدالية}}{=} \underbrace{x...x}_{n \text{ من المرات}} . \underbrace{y...y}_{n \text{ من المرات}}$$

$$= x^n y^n = e.e = e \Rightarrow xy\in H$$

(لاحظ أن : $((y^n)^{-1} = \underbrace{(y...y)^{-1}}_{n \text{ من المرات}} = \underbrace{y^{-1}...y^{-1}}_{n \text{ من المرات}} = (y^{-1})^n$)

مثال ١٠ : برهن أو انف :

(أ) $(\mathbb{R}\setminus\{0\},.) \hookrightarrow (H,.)$ $(H := \{x\in\mathbb{R}\setminus\{0\} \mid x=1 \vee x$ (غير نسبى)(عدد غير كسرى) $\})$

(ب) $(\mathbb{R}\setminus\{0\},.)$ $(K := \{x\in\mathbb{R}\setminus\{0\} \mid x\geq 1\})$ $(\mathbb{R}\setminus\{0\},.) \hookrightarrow (K,.)$

الحل: (أ) تقرير خاطئ . $\sqrt{2}\in H$ ، لكن $2 = \sqrt{2}.\sqrt{2}\notin H$

(ب) تقرير خاطئ . $2\in K$ لكن $2^{-1} = \frac{1}{2}\notin K$

مثال ١١ : لتكن G زمرة إبدالية ، e عنصرها المحايد وعليها العملية "." "الضرب" .

ولتكن $H := \{x^2 \mid x\in G\}$. برهن على أن H زمرة جزئية فى G .

البرهان :

$$e\in G \Rightarrow e = e^2 \in H$$

$$x^2\in H \Rightarrow x\in G \Rightarrow x^{-1}\in G \Rightarrow (x^2)^{-1} = (x^{-1})^2 \in H$$

$$x^2, y^2\in H \Rightarrow x\in G, y\in G \underset{G \text{ زمرة}}{\Rightarrow} xy\in G \Rightarrow x^2y^2 \underset{G \text{ إبدالية}}{=} (xy)^2\in H$$

$$\Rightarrow H \hookrightarrow G$$

مثال ١٢ : برهن على أن أية زمرة ذات ستة عناصر لايمكن أن تحتوى على زمرة جزئية ذات أربعة عناصر .

البرهان : لتكن G زمرة ذات ستة عناصر ، H زمرة جزئية من G ذات أربعة عناصر. لتكن $x\in G$ ، $x\notin H$. نكون $xH:=\{xh|h\in H\}$. واضح أن $xH\cap H=\phi$:
إذا كان $xH\cap H\neq\phi$ إذن يوجد g و z بحيث إن $z=xg\in xH, z,g\in H$ وهذا يقتضى أن : $x=zg^{-1}\in H$ تناقض . ولكن $H\subset G$ ، $xH\subset G$ وعدد عناصر xH يساوى عدد عناصر H (إذا كان عدد عناصر xH أقل من عدد عناصر H فمعنى هذا أنه يوجد $g_1,g_2\in H$ ، $g_1\neq g_2$ بحيث إن $xg_1=xg_2$ ولكن هذا يستلزم أن : $g_1=g_2$).
إذن عدد عناصر H+ عدد عناصر $xH=8$ تناقض (عدد عناصر $G=6$) .
(بصفة عامة عدد عناصر أى زمرة جزئية يكون قاسماً لعدد عناصر الزمرة . سنرى هذا فى نظرية لاجرانج) .

مثال ١٣ : لتكن $G:=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} | a,b,c,d\in\mathbb{Z}\right\}$ وعليها عملية جمع المصفوفات .

برهن على ان $H:=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} | a+b+c+d=0\right\}$ مع عملية جمع المصفوفات تكون زمرة جزئية من G . ماذا يحدث إذا استبدلنا 1 بـ 0 ؟.

الحـل :

$\begin{pmatrix} 0 & 0 \\ 0 & 0\end{pmatrix}\in H$. إذن H ليست خالية . ليكن $\begin{pmatrix} e & f \\ g & h\end{pmatrix},\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in H$ ينتج أن

$a+b+c+d=0$, $e+f+g+h=0$ والآن :

$$\begin{pmatrix} a-e & b-f \\ c-g & d-h\end{pmatrix}=\begin{pmatrix} a & b \\ c & d\end{pmatrix}-\begin{pmatrix} e & f \\ g & h\end{pmatrix}\in H$$ لأن :

$$a-e+b-f+c-g+d-h=a+b+c+d-(e+f+g+h)=0$$

ينتج أن $(H,+)$ زمرة جزئية من $(G,+)$. إذا استبدلنا ١ بـ ٠ لن يوجد العنصر $\begin{pmatrix} 0 & 0 \\ 0 & 0\end{pmatrix}$ فى H وهو شرط ضرورى حتى تكون H زمرة جزئية من G .

مثال ١٤ : لتكن $G := GL(2,\mathbb{R})$ (مجموعة المصفوفات من النوع 2×2 ومحددها لايساوى الصفر، عناصرها (مداخلها) من $\mathbb{R}$ ، **تسمى الزمرة الخطية العامة** (The general linear group). ولتكن $H := \{A\in G \mid \det(A) = 2^n, n\in \mathbb{Z}\}$. برهن على أن H زمرة جزئية من G .

البرهان :

$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\in H$ لأن $\det\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = 1 = 2^0$ ، ليكن

$$\det(A) = 2^n, \det(B) = 2^m, n,m\in \mathbb{Z} \Leftarrow A,B\in H$$

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)(\det(B))^{-1} = 2^n.2^{-m} = 2^{n-m}, n-m\in \mathbb{Z}$$

أى أن $AB^{-1}\in H$.

مثال ١٥ : لتكن H زمرة جزئية من $\mathbb{R}$ مع عملية الجمع ، $K := \{2^a \mid a\in H\}$. برهن على أن K زمرة جزئية من $\mathbb{R}\setminus\{0\}$ مع عملية الضرب .

البرهان : $0\in H$ ، $1 = 2^0\in K$. كذلك فإن : $2^a, 2^b\in K$ حيث $a,b\in H$ يقتضى أن : $2^a(2^b)^{-1} = 2^{a-b}\in K$ (لأن $a-b\in H$) أى أن K زمرة جزئية من $\mathbb{R}\setminus\{0\}$ مع عملية الضرب .

مثال ١٦ :

لتكن $G := GL(2,\mathbb{R})$ ، $H := \left\{\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix} \mid a,b\in \mathbb{Z}\setminus\{0\}\right\}$. برهن أو انف : H زمرة جزئية من G .

الحـل : العنصر المحايد فى G هو $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ فإذا كانت H زمرة جزئية من G فإن $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ يقع فيها كعنصر. لكن $\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}\in H$ ، بينما معكوسه $\begin{pmatrix}2^{-1} & 0\\ 0 & 2^{-1}\end{pmatrix}\notin H$. إذن H ليست زمرة جزئية من G .

مثال ١٧ : لتكن $H := \{a+bi \mid a,b\in \mathbb{R}, ab\geq 0\}$. برهن أو انف : H زمرة جزئية من $\mathbb{C}$ تحت عملية الجمع .

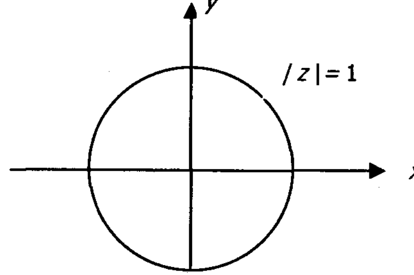
<u>الحــل</u>: $2+5i\in H$ ، $-3-i,$ بينما $-1+4i=(-3-i)+(2+5i)\notin H$ إذن H ليست زمرة جزئية من $\mathbb{C}$ تحت عملية الجمع .

<u>مثال ١٨</u> : لتكن $H:=\{a+bi\,|\,a,b\in\mathbb{R},a^2+b^2=1\}$. برهن أو انف : H زمرة جزئية من $\mathbb{C}\setminus\{0\}$ مع عملية الضرب . صف عناصر H هندسياً .

<u>الحل</u> : $1+0i\in H$ لأن $1^2+0^2=1$ ، وهو العنصر المحايد فى $(\mathbb{C}\setminus\{0\},.)$.

كذلك ليكن $a+bi=\cos\theta+i\sin\theta$ (لأن $a^2+b^2=1$) ، $c+di=\cos\varphi+i\sin\varphi$ عنصرين فى H ينتج ان $(a+bi)(c+di)=\cos(\theta+\varphi)+i\sin(\theta+\varphi)\in H$

وإذا كان $a+bi=\cos\theta+i\sin\theta$ عنصراً فى H فإن معكوسه هو $\cos(-\theta)+i\sin(-\theta)$ وهو كذلك عنصر فى H .



عناصر H هى جميع نقط الدائرة $x^2+y^2=1$ أى الدائرة $|z|=1$.

<u>طريقة أخرى</u> : واضح أن: $1+0i\in H$

ليكن $a+bi\in H$. معكوس $a+bi$ هو $(a+bi)^{-1}$

$$(a+bi)^{-1}=\frac{a-bi}{a^2+b^2},\left(\frac{a}{a^2+b^2}\right)^2+\left(\frac{-b}{a^2+b^2}\right)^2=\frac{a^2}{(a^2+b^2)^2}+\frac{b^2}{(a^2+b^2)^2}$$

$$=\frac{a^2+b^2}{(a^2+b^2)^2}=\frac{1}{a^2+b^2}=1\Rightarrow(a+bi)^{-1}\in H$$

والآن ليكن $a+bi,c+di\in H \quad\Leftarrow\quad a^2+b^2=1,c^2+d^2=1$

$$(a+bi)(c+di)=ac-bd+i(ad+bc),$$

$$(ac-bd)^2+(ad+bc)^2=a^2c^2-2acbd+b^2d^2+a^2d^2+2adbc+b^2c^2$$

$$=a^2c^2+b^2d^2+a^2d^2+b^2c^2$$

$$=(a^2+b^2)c^2+(b^2+a^2)d^2=c^2+d^2=1$$

$\Rightarrow(a+bi)(c+di)\in H\Rightarrow$ H زمرة جزئية من $(\mathbb{C}\setminus\{0\},.)$

١-٥ المجموعات المشاركة Cosets

١-٥-١ تعريف : لتكن G زمرة ، H زمرة جزئية من G، $a\in G$. تعرف المجموعة $aH:=\{ah \mid h\in H\}$ بأنها **المجموعة المشاركة اليسرى** من a بالنسبة إلى H (The left coset of a w.r.t. H) . كذلك المجموعة $Ha:=\{ha \mid h\in H\}$ هى **المجموعة المشاركة اليمنى** من a بالنسبة إلى (The right coset of a w.r.t. H) .

١-٥-٢ تمهيدية : لتكن G زمرة ، H زمرة جزئية من G . وليكن $a,b\in G$. التقريرات الآتية متكافئة :

(أ) $aH=bH$

(ب) $b\in aH$

(جـ) $a^{-1}b\in H$

وتوجد تقريرات مكافئة مناظرة للمجموعات المشاركة اليمنى من a بالنسبة إلى H .

البرهان : " (أ) $\Leftarrow$ (ب)" :

$$b=be\in bH=aH$$

" (ب) $\Leftarrow$ (جـ)" :

$$b\in aH\Rightarrow \exists h\in H: b=ah$$
$$\Rightarrow \exists h\in H: a^{-1}b=a^{-1}(ah)=(a^{-1}a)h=eh=h\in H$$

" (جـ) $\Leftarrow$ (أ)": "$\supset$" :

$$a^{-1}b\in H\Rightarrow \exists h\in H: a^{-1}b=h\in H\Rightarrow \exists h\in H: b=ah \qquad (1)$$
$$x\in bH\Rightarrow \exists k\in H: x=bk\underset{(1)}{=}ahk\in aH\Rightarrow bH\subset aH \qquad (2)$$

"$\subset$"

$$x\in aH\Rightarrow \exists \ell\in H: x=a\ell.$$

ومن (1) لدينا $a=bh^{-1}, h^{-1}\in H$ ($h\in H\Leftarrow h^{-1}\in H$ لأن H زمرة جزئية من G).
وبالتالى فإن : $x=bh^{-1}\ell\in bH$ وينتج مباشرة أن

$$aH\subset bH \qquad (3)$$

من (2) ، (3) ينتج المطلوب مباشرة .

١-٥-٣ تعريف : لتكن G زمرة . ولتكن H زمرة جزئية من G. وليكن $a,b\in G$. يقال إن

a مطابق لـ b مقياس H (a congruent to b modulo H): بالرموز $a \equiv b \bmod H$ عندما يتحقق شرط (وبالتالى كل الشروط) فى (١-٥-٢) .

١-٥-٤ ملحوظة : لتكن G زمرة ، ولتكن H زمرة جزئية من G. عندئذ فإن العلاقة "مطابق مقياس H" هى علاقة تكافؤ على G . ولكل $a \in G$ فإن aH هو فصل تكافؤ a .

البرهــان: لكل $aH = aH : a \in G \Leftarrow a \equiv a \bmod H$ أى أن العلاقة انعكاسية (reflexive).

$\forall a,b \in G : a \equiv b \bmod H \Rightarrow aH = bH \Rightarrow bH = aH \Rightarrow b \equiv a \bmod H$

أى أن العلاقة متماثلة (symmetric) .

$\forall a,b,c \in G : a \equiv b \bmod H, b \equiv c \bmod H \Rightarrow aH = bH, bH = cH$

$\Rightarrow aH = cH \Rightarrow a \equiv c \bmod H$

أى أن العلاقة انتقالية (transitive) ومن ثم فهى علاقة تكافؤ (equivalence relation) .

١-٥-٥ مثال : لكل $m \in \mathbb{Z}$ تكون $m\mathbb{Z}$ زمرة جزئية من $\mathbb{Z}$ (بالنسبة للعملية +). فى حالة $m \neq 0$ لكل $k, \ell \in \mathbb{Z}$:

$$k \equiv \ell \bmod m\mathbb{Z} \Leftrightarrow \ell - k \in m\mathbb{Z}$$

$\ell - k$ يقبل القسمة بدون باق على $m \Leftrightarrow$

k, ℓ لهما نفس باقى القسمة الموجب من خلال القسمة على $m \Leftrightarrow$

وإذا كان $k \in \mathbb{Z}$ ، r باقى القسمة الموجب من قسمة k على m فإن :

$$k + m\mathbb{Z} = r + m\mathbb{Z}$$

وتكون $\{r + m\mathbb{Z} : r \in \mathbb{N}, 0 \leq r < |m|\}$ هى مجموعة المجموعات المشاركة اليسرى لعناصر $\mathbb{Z}$ بالنسبة إلى $m\mathbb{Z}$.

١-٥-٦ تمهيدية : لتكن G زمرة ، H زمرة جزئية من G . لتكن G/H مجموعة المجموعات المشاركة اليسرى ، $G \backslash H$ مجموعة المجموعات المشاركة اليمنى بالنسبة إلى H . يوجد تناظر أحادى:

$$f : G/H \to G \backslash H$$
$$aH \mapsto Ha^{-1}$$

البرهان : سنثبت اولاً أن **الراسم معرف جيداً** (well-defined) . رأينا فى (١-٥-٢) أنه قد يوجد $a, b \in G$ ، $a \neq b$ بينما $aH = bH$ حيث H زمرة جزئية فى G .

وحتى يكون الراسم معرفاً جيداً ينبغى أن نثبت أنه إذا كان $aH = bH$ فإن $Ha^{-1} = Hb^{-1}$، وذلك كالآتى : $bH = aH$ يقتضى أنه يوجد $x \in H$ بحيث يكون $b = ax$. ومن ثم فإن $b^{-1} = x^{-1}a^{-1} \in Ha^{-1}$ وبالتالى فإن $Hb^{-1} = Ha^{-1}$ (التقريرات المناظرة للتقريرات فى (١-٥-٢)) .

واضح أن الراسم غامر(شامل). لإثبات أن الراسم واحد لواحد: ليكن $Ha^{-1} = Hb^{-1}$ ينتج أن $a^{-1} = hb^{-1}$ حيث $h \in H$ ، ومن ثم فإن $a^{-1}b \in H$ ومن (١-٥-٢) ينتج أن $aH = bH$. أى أن الراسم واحد لواحد.

١-٦ الزمر الجزئية الطبيعية Normal subgroups

١-٦-١ تمهيدية: لتكن G زمرة ، H زمرة جزئية من G . التقريرات الآتية متكافئة :

(١) $aH = Ha$ لجميع $a \in G$

(٢) $aHa^{-1} \subset H$ لجميع $a \in G$

(٣) $\varphi(H) \subset H$ لجميع الأوتومورفيزمات الداخلية φ من G .

(٤) $aHa^{-1} = H$ لجميع $a \in G$

(٥) $\varphi(H) = H$ لجميع الأوتومورفيزمات الداخلية φ من G .

البرهان : "(١) $\Rightarrow$ (٢)" :

$$x \in aHa^{-1} \Rightarrow \exists h \in H : x = aha^{-1}.\ aH = Ha \Rightarrow \exists \ell \in H : ah = \ell a$$

$$\Rightarrow x = aha^{-1} = \ell aa^{-1} = \ell \in H \Rightarrow aHa^{-1} \subset H$$

"(٢) $\Leftrightarrow$ (٣)" : ينتج مباشرة من تعريف الأوتومورفيزم الداخلى.

"(٣) $\Rightarrow$ (4)": $\varphi(H) \subset H$ لجميع الأوتومورفيزمات الداخلية $\varphi \Rightarrow \forall a \in G : aHa^{-1} \subset H$

$$\underset{(a^{-1})^{-1}=a}{\Rightarrow} \forall a \in G : a^{-1}Ha \subset H \Rightarrow \forall a \in G : H \subset aHa^{-1} \Rightarrow \forall a \in G : aHa^{-1} = H$$

طريقة أخرى : φ أوتومورفيزم داخلى من G ينتج عنه أن φ^{-1} أيضاً أوتومورفيزم داخلى من G بحيث يكون $\varphi(H) \subset H$ ، $\varphi^{-1}(H) \subset H$ ، وبالتالى فإن : $\varphi(H) \subset H$ ، $H = \varphi(\varphi^{-1}(H)) \subset \varphi(H)$. ينتج أن $aHa^{-1} = \varphi(H) = H$ لكل $a \in G$.

"(٤) $\Leftrightarrow$ (٥)" : واضح

"(٤) $\Rightarrow$ (1)" : $x \in aH \Rightarrow$ يوجد $h \in H$ بحيث إن $x = ah$.

$aHa^{-1}=H$ ⇐ يوجد $\ell\in H$ بحيث إن $aha^{-1}=\ell$ ⇐ يوجد $\ell\in H$ بحيث إن

$$xa^{-1}=\ell\in H \Leftarrow x=\ell a\in Ha \Leftarrow aH\subset Ha \qquad (*)$$

$x\in Ha$ ⇐ يوجد $h\in H$ بحيث يكون $aHa^{-1}=H.x=ha$ ⇐ يوجد

$\ell\in H$ بحيث إن: $a\ell a^{-1}=h$ ومن ثم فإنه يوجد $\ell\in H$ بحيث إن

$$x=ha=a\ell\in aH \Leftarrow Ha\subset aH \qquad (**)$$

من (*) ، (**) ينتج أن $aH=Ha$.

<u>١-٦-٢ تعريف</u> : الزمرة الجزئية H من الزمرة G تسمى <u>زمرة جزئية طبيعية</u> (normal subgroup) إذا حققت شرطاً (ومن ثم كل الشروط) فى (١-٦-١) .

<u>١-٦-٣ أمثلة</u> : (١) كل زمرة G تحتوى على زمرتين جزئيتين طبيعيتين تافهتين هما G نفسها ، $\{e\}$ ، (حيث e هو عنصر G المحايد) .

(٢) كل زمرة جزئية من زمرة إبدالية G تكون زمرة جزئية طبيعية من G .

<u>١-٦-٤ ملحوظة</u>: ليكن $\varphi:G\to G'$ هومومورفيزم زمر من الزمرة G إلى الزمرة G' .

(أ) لكل N' زمرة جزئية طبيعية من G' يكون $\varphi^{-1}(N')$ زمرة جزئية طبيعية من G . وعلى وجه الخصوص $Ker(\varphi)$ زمرة جزئية طبيعية من G .

(ب) إذا كان φ راسماً غامراً (فوقياً) ، N زمرة جزئية طبيعية من G ، فإن $\varphi(N)$ يكون زمرة جزئية طبيعية من G' .

<u>البرهـــان</u> : (أ) من (١-٤-٣) $\varphi^{-1}(N')$ زمرة جزئية من G . والآن لكل $a\in G$ ولكل $x\in\varphi^{-1}(N')$:

$$\varphi(axa^{-1}) = \varphi(a)\varphi(x)\varphi(a^{-1}) = \varphi(a)\varphi(x)\varphi(a)^{-1}\in\varphi(a)N'\varphi(a)^{-1}\subset N'$$

φ هومومورفيزم ١-٣-٢ N' زمرة جزئية طبيعية فى G'

$$\Rightarrow axa^{-1}\in\varphi^{-1}(N') \Rightarrow$$ $\varphi^{-1}(N')$ زمرة جزئية طبيعية فى G

(ب) ليكن $x'\in\varphi(N)$ ، $a'\in G'$. يوجد $x\in N$ بحيث إن $\varphi(x)=x'$. ولأن φ راسم فوقى (شامل) فإنه يوجد $a\in G$ بحيث إن $\varphi(a)=a'$. والآن :

$$a'x'a'^{-1}=\varphi(a)\varphi(x)\varphi(a)^{-1} = \varphi(a)\varphi(x)\varphi(a^{-1}) = \varphi(axa^{-1})\in\varphi(N)$$

φ هومومورفيزم ١-٣-٢

N زمرة جزئية طبيعية من G

١-٦-٥ مثال : ليكن $\varphi: G \to G'$ هومومورفيزم زمر . φ ليس راسماً شاملاً (غامراً). N زمرة جزئية طبيعية فى G . $\varphi(N)$ ليست بالضرورة زمرة جزئية طبيعية فى G' .

سنأخذ H زمرة جزئية فى G لكنها ليست زمرة جزئية طبيعية فيها .

راسم التضمين $\iota: H \hookrightarrow G$ هومومورفيزم لأن :

$$a \mapsto a$$

$$\forall a,b \in H : \iota(ab) = ab = \iota(a)\iota(b)$$

H زمرة جزئية طبيعية فى نفسها (زمرة جزئية طبيعية تافهة) لكن $\iota(H) = H$ ليست زمرة جزئية طبيعية فى G .

ويمكن تكوين أمثلة عديدة لهذا: خذ مثلاً $G = \gamma_3$ ، $H = \{e,(12)\}$ (e هو العنصر المحايد فى G). H زمرة جزئية من γ_3 ، لكنها ليست زمرة جزئية طبيعية فيها :

$$(13)(12)(13) = (23) \notin \{e,(12)\}$$

١-٦-٦ تعريف : لتكن G زمرة ، H زمرة جزئية من G . تسمى المجموعة

$$Nor(H) := \{a \in G : aHa^{-1} = H\}$$

مطبع H (Normalizer) فى G .

١-٦-٧ ملحوظة : لتكن G زمرة ، H زمرة جزئية من G، $Nor(H)$ مطبع H فى G . عندئذ فإن :

(١) $Nor(H)$ زمرة جزئية من G .

(٢) H زمرة جزئية طبيعية من $Nor(H)$

(٣) إذا كانت K زمرة جزئية من G، H زمرة جزئية طبيعية من K فإن $K \subset Nor(H)$.

أى أن $Nor(H)$ هى أكبر زمرة جزئية فى G يكون فيها H زمرة جزئية طبيعية .

البرهان : (١) لكل $a \in G$ ليكن $\begin{matrix}\varphi_a : G \to G \\ x \mapsto axa^{-1}\end{matrix}$ هو الأوتومورفيزم الداخلى من G .

$$\Rightarrow \quad \forall a \in G : a \in Nor(H) \Leftrightarrow \varphi_a(H) = H \qquad (*)$$

والآن نبرهن على أن $Nor(H)$ زمرة جزئية من G . أولاً من الواضح أن e العنصر المحايد فى G يقع فى $Nor(H)$. ثانياً :

$a,b \in Nor(H) \Rightarrow \varphi_a(H) = H, \varphi_b(H) = H \Rightarrow \varphi_{ab}(H) = (\varphi_a o \varphi_b)(H) =$
$\varphi_a(\varphi_b(H)) = \varphi_a(H) = H \underset{(*)}{\Rightarrow} ab \in Nor(H)$

ثالثا : $a \in Nor(H) \Rightarrow \varphi_a(H) = H \Rightarrow \varphi_{a^{-1}}(H) = H \Rightarrow a^{-1} \in Nor(H)$

(٢) واضح من التعريف .

(٣) H زمرة جزئية طبيعية من $K \Leftarrow$ لكل $a \in K$: $aHa^{-1} = H \Leftarrow$ لكل $a \in K$:

$a \in Nor(H) \Leftarrow K \subset Nor(H)$

١-٧ الزمر العاملة Factor groups

<u>١-٧-١ نظرية</u> : لتكن G زمرة ، N زمرة جزئية طبيعية فى G، G/N مجموعة كل المجموعات المشاركة اليسرى من G بالنسبة إلى N ، $\rho : G \to G/N$, $a \mapsto aN$

عندئذ فإنه يوجد بالضبط ربط واحد "." فى G/N بحيث يكون :

(أ) $(G/N, .)$ زمرة .

(ب) الراسم ρ هومومورفيزم من G إلى $(G/N, .)$.

ρ عندئذ يكون إبيمورفيزم ، $Ker(\rho) = N$ ، N هو العنصر المحايد فى $(G/N, .)$ ، $a^{-1}N$ هو معكوس aN .

<u>البرهان</u> : (١) وحدانية الربط (uniqueness) : إذا كانت $(G/N, .)$ زمرة ، ρ هومومورفيزم من G إلى $(G/N, .)$ فإنه لجميع $a,b \in G$:

$$aN.bN = \rho(a).\rho(b) = \rho(ab) = (ab)N$$

(٢) سنثبت أن الربط المعطى فى (١) معرف جيداً أى أنه موجود (exists) ونحن نعلم من (١-٥-٢) أنه قد يوجد عنصران $a,b \in G$ مختلفان وعلى الرغم من هذا يكون $aH = bH$ حيث H زمرة جزئية فى الزمرة G .

ولهذا فإنه حتى نثبت أن الربط معرف جيداً فإننا نثبت أنه إذا كان $aN = a'N$ ، $bN = b'N$ حيث $a, a', b, b' \in G$ فإن $abN = a'b'N$ (ويقال إن الربط لايعتمد على الممثل (The representative). سنكتب $N \lhd G$ إذا كانت N زمرة جزئية طبيعية فى الزمرة G .

نلاحظ أولاً أنه إذا كان $n\in N \lhd G$ ، $b'\in G$ فإن : $nb'=b'\ell$ حيث $\ell\in G$

(لأن $N \lhd G$ تعنى أنه لكل $a\in G$: $aN=Na$) (1')

ونلاحظ ثانياً أنه إذا كان $a\in H$ حيث H زمرة جزئية من G فإن $aH=H$ حيث $a\in G$.

(لأن: $H=aH \Leftrightarrow eH=aH \Leftrightarrow e^{-1}a\in H \Leftrightarrow a\in H$) (2')

١-٥-٢

باستخدام هاتين الملاحظتين سنثبت أن الربط المعطى فى (١) معرف جيداً كالآتى :

ليكن :

$$\begin{aligned} &aN=a'N, bN=b'N, a,a',b,b'\in G\\ &\Rightarrow \exists n,m\in N: a=a'n, b=b'm\\ &\Rightarrow abN=a'nb'mN \underset{(1')}{=} a'b'\ell mN \underset{(2')}{=} a'b'N, \ell\in N \end{aligned}$$

والآن

$$\begin{aligned} \forall a,b,c\in G: (aN.bN).cN &= (abN).cN=(ab)cN\\ &= a(bc)N=aN.bcN=aN.(bN.cN) \end{aligned}$$

كذلك

$$\forall a\in G: N.aN=eN.aN=eaN=aN$$

أى أن N هو العنصر المحايد فى $(G/N,.)$

$$\forall a\in G: \quad a^{-1}N.aN=a^{-1}aN=eN=N$$

أى أن $a^{-1}N$ هو معكوس aN .

واضح أن ρ راسم فوقى (شامل) وبالتالى فإنه إبيمورفيزم

نواة (ρ) $\quad Ker(\rho)=\{a\in G:\rho(a)=N\}=\{a\in G: aN=N\}$

$$=\{a\in G: a\in N\}=N$$

<u>١-٧-٢ تعريف</u> :G زمرة ، N زمرة جزئية طبيعية فى G. تسمى الزمرة المنشأة فى (١-٧-١)<u>الزمرة العاملة(أو زمرة القسمة)لــ G مقياس N</u> . يسمى الإبيمورفيزم $\rho: G\to G/N$ <u>الإبيمورفيزم الطبيعى</u>(The canonical epimorphism) لــ G على G/N .

$$a\mapsto a/N$$

<u>١-٧-٣ ملحوظة</u> : لتكن G زمرة ، N مجموعة جزئية من G .
N زمرة جزئية طبيعية من G إذا وفقط إذا وجدت زمرة G' ، ووجد هومومورفيزم $\varphi : G \to G'$ بحيث يكون $Ker(\varphi) = N$.

<u>البرهان</u> : "$\Leftarrow$" : ينتج من النظرية (١-٧-١)

"$\Rightarrow$" : ينتج كذلك مباشرة من (١-٦-٤) (أ)

<u>١-٧-٤ مثال</u> : الزمرة$(\mathbb{Z},+)$ إبدالية، ومن ثم فإن أية زمرة جزئية منها تكون زمرة جزئية طبيعية. ولهذا فإنه لأى $m \in \mathbb{Z}$ يكون لدينا الزمرة $\mathbb{Z}/m\mathbb{Z}$ ويكون الحساب فى $\mathbb{Z}/m\mathbb{Z}$ كالآتى :

$$\forall k, \ell \in \mathbb{Z} : (k + m\mathbb{Z}) + (\ell + m\mathbb{Z}) = (k + \ell) + m\mathbb{Z}$$

فى حالة $m = 0$ يكون $\mathbb{Z}/m\mathbb{Z} = \{\{k\} : k \in \mathbb{Z}\}$

(ويكتب أحياناً $\mathbb{Z}/m\mathbb{Z} = \{\bar{k} : k \in \mathbb{Z}\}$)

$$= \{k + m\mathbb{Z} : k \in \mathbb{Z}\}$$

ويكون الراسم :

$$\rho : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$
$$k \mapsto \{k\} = k + m\mathbb{Z}$$

أيزومورفيزم زمر .

فى حالة $m \neq 0$ تكون $\mathbb{Z}/m\mathbb{Z}$ زمرة عدد عناصرها $|m|$ وهى :

$k + m\mathbb{Z}, k \in \{0, \ldots, |m| - 1\}$ (انظر مثال (١-٥-٥))

<u>وسنكتب أحياناً $\mathbb{Z}_m$ لنعنى $\mathbb{Z}/m\mathbb{Z}$</u>

١-٨ نظريات الأيزومورفيزم The Isomorphism Theorems

١-٨-١ نظرية الهومومورفيزم The Homomorphism Theorem

ليكن $f : G \to G'$ هومومورفيزم زمر من الزمرة G إلى الزمرة G'

$$\Rightarrow \quad G/Ker(f) \cong f(G)$$

أى أن كل هومومورفيزم ينتج عنه أيزومورفيزم

البرهان : سنضع الراسم من $G/Ker(f)$ إلى $f(G)$ ونثبت أنه أيزومورفيزم كالآتى :

$$\varphi : G/Ker(f) \to f(G)$$
$$aKer(f) \mapsto f(a)$$
$$\forall a \in G : \varphi(aKer(f)) := f(a)$$

(١) الر اسم φ معرف جيداً: لكل $a,b \in G$ ليكن $aKer(f) = bKer(f)$ ينتج من (١-٥-٢) أن :

$$a^{-1}b \in Ker(f) \Rightarrow f(a)^{-1} f(b) = f(a^{-1}) f(b) = f(a^{-1}b) = e'$$ (e' العنصر المحايد فى G')

١-٣-٢

$$\Rightarrow f(a) = f(b)$$

أى أن : $\varphi(aKer(f)) = \varphi(bKer(f))$ وبهذا يكون الراسم معرفاً جيداً لأنه لايعتمد على الممثل (The representative) .

(٢) φ راسم فوقى (شامل) : واضح (لأن كل عنصر فى $f(G)$ سيكون على الشكل $f(a)$ وبالتالى فإنه يوجد $aKer(f) \in G/Ker(f)$ بحيث يكون $\varphi(aKer(f)) = f(a)$.

(٣) φ واحد لواحد : ليكن $\forall a,b \in G : \varphi(aKer(f)) = \varphi(bKer(f))$ ، أى أن $f(a) = f(b)$.

ينتج أن :

$$f(a^{-1}b) = f(a^{-1}) f(b) = f(a)^{-1} f(b) = e' \Rightarrow a^{-1}b \in Ker(f)$$

١-٣-٢

$$\Rightarrow aKer(f) = bKer(f)$$

١-٥-٢

(٤) φ هومومورفيزم :

$$\forall a,b \in G : \varphi(aKer(f).bKer(f)) = \varphi(abKer(f))$$

١-٧-١

(تذكر أن $Ker(f)$ زمرة جزئية طبيعية من G (١-٦-٤))

$$= f(ab) = f(a) f(b) = \varphi(aKer(f))\varphi(bKer(f))$$

١-٨-٢ النظرية الأولى للأيزومورفيزم The First Isomorphism Theorem

ليكن $f:G \to G'$ هومومورفيزم زمر من الزمرة G إلى الزمرة G' .

لتكن $U \hookrightarrow G$ (زمرة جزئية من G) ، $N \lhd G$ (زمرة جزئية طبيعية من G) .

$$\Rightarrow U/_{U \cap N} \cong UN/_N$$

حيث $UN := \{un / u \in U, n \in N\}$

البرهان :

سنثبت أولاً أن UN زمرة جزئية من G حتى يكون للادعاء معنىً .

e العنصر المحايد فى G موجود فى U، N وبالتالى فإن $e = e.e \in UN$ ، وبالتالى فإن $UN \neq \phi$. والآن ليكن $u_1n_1, u_2n_2 \in UN$:

$$u_1n_1.u_2n_2 = u_1u_2n_3n_2 \in UN, n_3 \in N$$

(راجع (١-٦-١)) .

كذلك فإن :

$$\forall un \in UN : (un)^{-1} = n^{-1}u^{-1} = u^{-1}n' \in UN, n' \in N$$

أى أن UN زمرة جزئية فى G .

والآن $\forall n \in N : n = en \in UN$ أى أن $N \subset UN$ ، N زمرة جزئية طبيعية فى G ومن ثم فهى زمرة جزئية طبيعية من UN ، ويكون للكتابة $UN/_N$ معنى : فهى زمرة .

والآن إذا كان الادعاء صحيحاً فإن $U/_{U \cap N}$ يجب أن تكون زمرة وهذا يقتضى أن يكون $(U \cap N) \lhd U$. ويمكن بسهولة البرهنة على هذا ثم إثبات الأيزومورفيزم لكننا نفضل أن نجرى الآتى:

نعرف الراسم φ كما يلى :

$$\varphi : U \to UN/_N$$

$$a \mapsto aN$$

واضح أن φ معرف جيداً ، وواضح أنه راسم فوقى (شامل) . والآن :

$$\forall a,b \in U : \varphi(ab) = abN = aN.bN = \varphi(a)\varphi(b)$$

أى أن φ هومومورفيزم. ونحسب نواة (φ) :

$$Ker(\varphi)=\{a\in U:\varphi(a)=N\}$$
$$=\{a\in U:aN=N\}=\{a\in U:a\in N\}=U\cap N$$

أى أن $U\cap N$ زمرة جزئية طبيعية فى U(١-٦-٤ (أ))

والآن نطبق نظرية الهومومورفيزم (١-٨-١) :

$$U/U\cap N=U/Ker(\varphi)\cong\varphi(U)\quad=\quad UN/N$$

φ شامل .

نهاية البرهان .

١-٨-٣ النظرية الثانية للأيزومورفيزم The Second Isomorphism Theorem

لتكن G زمرة ، M,N زمرتين جزئيتين طبيعيتين فى G، $N\subset M$. ينتج أن:

$$G/N\big/M/N\cong G/M$$

البرهان : حتى يكون للادعاء معنىً يجب أن يكون M/N زمرة جزئية طبيعية فى G/N لكننا لن نفعل هذا بصورة منفردة ، بل سنتتبع الآتى :

نعرف الراسم φ :

$$\varphi:G/N\to G/M$$
$$aN\mapsto aM$$

(١) φ معرف جيداً :

$$\forall a,b\in G:aN=bN\;\underset{1-6-1}{\Rightarrow}\;a^{-1}b\in N\underset{N\subset M}{\Rightarrow}a^{-1}b\in M$$

$$\underset{1-6-1}{\Rightarrow aM=bM}$$

(٢) φ راسم غامر (شامل) : واضح

(٣) φ هومومورفيزم :

$$\forall a,b\in G:\varphi(aN.bN)\;\underset{1-7-1}{=}\;\varphi(abN)=abM\;\underset{1-7-1}{=}\;aM.bM$$
$$=\varphi(aN)\varphi(bN)$$

(٤) نواة (φ):

$$Ker(\varphi)=\{aN\in {G}/{N}:\varphi(aN)=M\}$$
$$=\{aN\in {G}/{N}:aM=M\}=\{aN\in {G}/{N}:a\in M\}={M}/{N}$$

أى أن M/N زمرة جزئية طبيعية فى G/N (١-٦-٤)

والآن نطبق نظرية الهومومورفيزم (١-٨-١) :

$$\frac{G/N}{M/N}=\frac{G/N}{Ker(\varphi)}=\varphi(G/N) \;=\; G/M$$

φ شامل

نهاية البرهان .

١-٩ النوايا المرتبيه والنوايا المشاركة المرتبية

Categorical Kernels & Categorical Cokernels

<u>١-٩-١ تعريف</u> : ليكن $f:G\to H$ هومومورفيزم زمر من الزمرة G إلى الزمرة H .

تسمى زمرة K مع هومورفيزم $g:K\to G$ **<u>نواة مرتبية</u>** (Cotegorical kernel) .

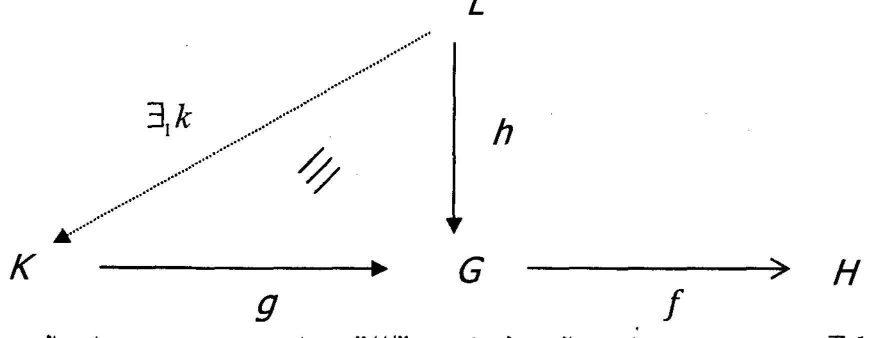
لـــ f إذا تحقق :

(١) $fg=1$ (أى أن $\forall a\in K:fg(a)=e_H$)

(e_H هو العنصر المحايد فى H، fg تعنى fog وهكذا فى باقى التركيبات) .

(٢) لكل زمرة L ، لكل $h:L\to G$ هومومورفيزم زمر :

$[fh=1\Rightarrow \exists_1 k:L\to K$ هومومورفيزم $: h=gk]$



($\exists_1 k$ تعنى يوجد واحد بالضبط k . "///" داخل الرسم تعنى ان الرسم إبدالى (commutative) . فى الشكل المعطى معناه $gk=h$) .

١-٩-٢ نظرية : النوايا المرتبية موجودة ، وهى وحيدة بدون حساب النوايا المتشاكلة (unique up to isomorphism)

البرهان : الوجود : (Existence)

سنعرف K ، g كالآتى : $K := Ker(f)$ ، $g : Ker(f) \to G$ ، $x \mapsto x$

أى أن $g = \imath$ (راسم التضمين The inclusion mapping)

والآن

$$\forall x \in Ker(f) : (fg)(x) = f(g(x)) = f(x) = e_H$$

$fh = 1$ معناه : $\forall x \in L : (fh)(x) = e_H$ ، أى أن $\forall x \in L : f(h(x)) = e_H$. أى أن $h(x) \in Ker(f)$. ولهذا نعرف k كالآتى : $\forall x \in L : k(x) := h(x)$ ويكون بهذا k معرفاً جيداً لأن $k(x) \in K = Ker(f)$

$$\forall x \in L : (gk)(x) = g(k(x)) = \imath(h(x)) = h(x) \Rightarrow gk = h$$

k هومومورفيزم لأن h هومومورفيزم .

k وحيد لأنه بفرض وجود هومومورفيزم ℓ بحيث يكون $gk = g\ell$ فإن هذا معناه أن $\imath k = \imath \ell$ أى أن

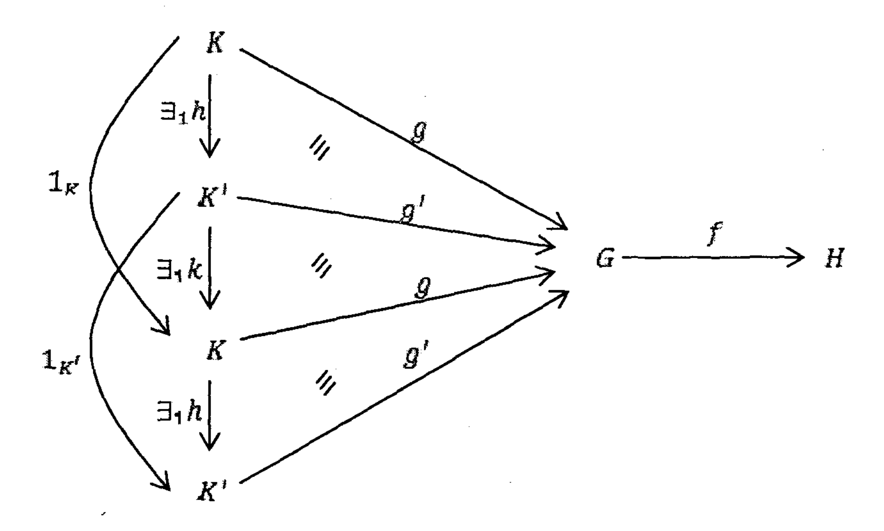
$$\forall x \in L : \imath(k(x)) = (\imath k)(x) = (\imath \ell)(x) = \imath(\ell(x))$$

$$\Rightarrow \quad \forall x \in L : k(x) = \ell(x) \Rightarrow k = \ell$$

$\imath$ مونومورفيزم

الوحدانية (Uniqueness)

ليكن K,g وكذلك K',g' نواة مرتبية . من حيث إن K,g نواة مرتبية لـــ f إذن $fg = 1$. ومن حيث إن K',g' نواة مرتبية لـــ f، K زمرة بحيث إن $fg = 1$. إذن يوجد هومومورفيزم وحيد $h : K \to K'$ بحيث إن $g'h = g$. والآن K',g' نواة مرتبية لـــ f إذن $fg' = 1$



ومن حيث إن K,g نواة مرتبية لـ f، K' زمرة بحيث إن $fg'=1$. إذن يوجد هومومورفيزم وحيد $k:K'\to K$ بحيث إن $gk=g'$. مرة ثالثة : من حيث إن K,g نواة مرتبية لـ f . إذن $fg=1$. ومن حيث إن K',g' نواة مرتبية لـ f، K زمرة بحيث إن $fg=1$. إذن يوجد هومورفيزم وحيد $h:K\to K'$ بحيث إن $g'h=g$. محصلة هذا أنه يوجد هومومورفيزم وحيد $koh:K\to K$ بحيث إن الشكل $KK'KG$ يكون إبدالياً. ولكن الهومومورفيزم $\begin{matrix}1_K:K\to K\\ a\mapsto a\end{matrix}$ يجعل نفس الشكل إبدالياً. ومن ثم فإن: $koh=1_K$ (1)

كذلك من المحصلة يوجد هومومورفيزم وحيد $hok:K'\to K'$ يجعل الشكل $K'KK'G$ إبدالياً. لكن الهومومورفيزم $\begin{matrix}1_{K'}:K'\to K'\\ \mathrm{b}\mapsto b\end{matrix}$ يجعل نفس الشكل إبدالياً .

ومن ثم فإن : $hok=1_{K'}$ (2) .

من (١) ينتج أن h مونومورفيزم ، k إبيمورفيزم . ومن (٢) ينتج أن k مونومورفيزم ، h إبيمورفيزم. وبالتالى فإن h (وكذلك k) أيزومورفيزم (تشاكل) وتكون النواة المرتبية وحيدة (بدون حساب النوايا المتشاكلة) .

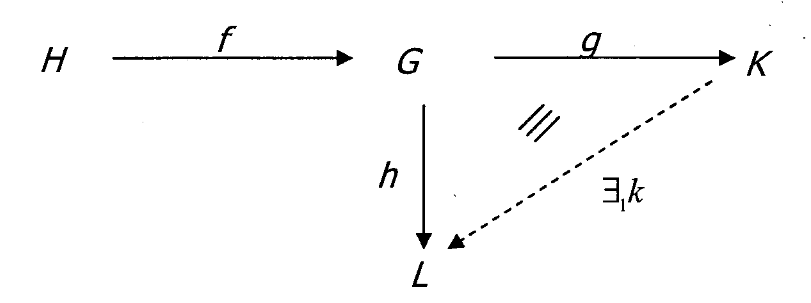
<u>**١-٩-٣ تعريف**</u> : ليكن $f:H\to G$ هومومورفيزم زمر من الزمرة H إلى الزمرة G . تسمى الزمرة K مع الهومومورفيزم $g:G\to K$ <u>**نواة مشاركة مرتبية**</u>

(Categorical Cokernel) لـــ f إذا تحقق :

(١) $gf=1$ (أى أن $\forall a\in H:(gf)(a)=e_K$)

(٢) لكل زمرة L ولكل $h:G\to L$ هومومورفيزم زمر :

$[hf=1\Rightarrow \exists_1 k:K\to L$ هومومورفيزم $: kg=h]$



١-٩-٤ نظرية : النوايا المشاركة المرتبية موجودة ، وهى وحيدة بدون حساب النوايا المشاركة المتشاكلة (unique up to isomorphism) .

البرهـــان : من (١-٤-٣) : صورة (f) زمرة جزئية من G: $\text{Im}(f)\hookrightarrow G$

والآن نكون B حيث $B:=\cap\{N\mid N\lhd G,\text{Im}(f)\subset N\}$

ومن مثال٦ فى (١-٤-٤) تقاطع زمرتين جزئيتين من زمرة A هو زمرة جزئية من A، ومن ثم فإن B زمرة جزئية من G . كذلك فإنه لكل $a\in G$ ، $b\in B$. $aba^{-1}\in N$ لجميع N (الزمر الجزئية الطبيعية فى G) ومن ثم فإن $aba^{-1}\in B$ أى أن B زمرة جزئية طبيعية فى G . والآن ننشئ $K:=G/B$ ، نعرف $\begin{array}{c}g:G\to G/B\\ a\mapsto aB\end{array}$ الإبيمورفيزم الطبيعى .

والآن : لكل $(gf)(x)=g(b)=B:x\in H$ (B هو العنصر المحايد فى G/B) ، ($b\in B$ لأن $b=f(x)\in\text{Im}(f)$ وبالتالى فإن $g(b)=bB=B$ كما ذكر هذا فى نظرية الزمر العاملة) أى أن $gf=1$.

والآن ليكن لدينا L، $h:G\to L$ هومومورفيزم بحيث إن $hf=1$. هذا يقتضى أن :

$h(\text{Im}(f))=\{e_L\}$ حيث e_L العنصر المحايد فى $L\Leftarrow$

$Ker(h) \supset \text{Im}(f)$, $Ker(h)$. زمرة جزئية طبيعية من H وبالتالى فإن $B \subset Ker(h)$.

نعرف $k(cB) := h(c)$ لجميع $c \in G$. نستطيع أن نثبت الآن أن k معرف جيداً كالآتى :

ليكن $cB = c'B$ لجميع $c, c' \in G$. هذا يستلزم أن

$$h(c) = h(c') \Leftarrow h(c^{-1}c') = e_L \Leftarrow c^{-1}c' \in B \subset Ker(h)$$

كذلك فإن k هومومورفيزم لأن :

$$\forall c, c' \in G : k(cB.c'B) = k(cc'B) = h(cc') = h(c)h(c')$$

h هومومورفيزم التعريف

$$= k(cB)k(c'B)$$

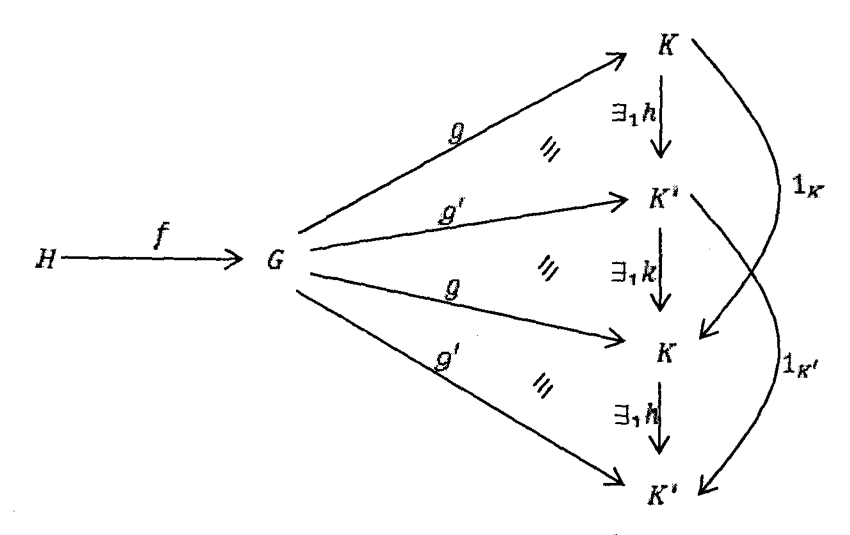
التعريف

نثبت كذلك أن $kg = h$ كالآتى :

$$\forall c \in G : (kg)(c) = k(g(c)) = k(cB) = h(c)$$

ونثبت وحدانية k : ليكن k', k بحيث إن $k'g = kg = h$. هذا معناه أن لكل $x \in G$: $(k'g)(x) = (kg)(x)$ أى أن $k'(g(x)) = k(g(x))$ ولكن g إبيمورفيزم فينتج أن $k' = k$.

<u>**وحدانية الحل**</u> :



طريقة البرهان تشبه تماماً الطريقة المتبعة فى حالة النوايا المرتبية .

من حيث إن K',g' حل أى نواة مشاركة مرتبية لـــ f إذن $g'f=1$. ومن حيث إن K,g نواة مشاركة مرتبية لـــ f، K زمرة بحيث إن $g'f=1$. إذن يوجد هومومورفيزم وحيد $h:K\to K'$ بحيث إن $hg=g'$.

والآن K,g نواة مشاركة مرتبية لـــ f . إذن $gf=1$. ومن حيث إن K',g' نواة مشاركة مرتبية لـــ f، K زمرة بحيث إن $gf=1$. إذن يوجد هومومورفيزم وحيد $k:K'\to K$ بحيث إن $kg'=g$. ومرة ثالثة : من حيث إن K',g' نواة مشاركة مرتبية لـــ f إذن $g'f=1$. ومن حيث إن K,g نواة مشاركة مرتبية لـــ f، K' زمرة بحيث إن $g'f=1$: إذن يوجد هومومورفيزم وحيد $h:K\to K'$ بحيث إن $hg=g'$. ومحصلة هذا أنه يوجد هومومورفيزم وحيد $koh:K\to K$ بحيث يكون الشكل $GKK'K$ إبدالياً . ولكن الهومومورفيزم $\begin{aligned}1_K:K&\to K\\ a&\mapsto a\end{aligned}$ يجعل الشكل إبدالياً كدذلك: إذن (1) $koh=1_K$. كذلك من محصلة النتائج السابقة أنه يوجد هومومورفيزم وحيد $hok:K'\to K'$ يجعل الشكل $GK'KK'$ إبدالياً . لكن الهومومورفيزم $\begin{aligned}1_{K'}:K'&\to K'\\ b&\mapsto b\end{aligned}$ يجعل الشكل نفسه كذلك إبداليا.. إذن (2) $hok=1_{K'}$.

من (1) ينتج أن h مونومورفيزم ، k إبيمورفيزم . ومن (2) ينتج أن k مونومورفيزم ، h إبيمورفيزم. وبالتالى فإن h، k أيزومورفيزمان وتكون النواة المشاركة المرتبية لـــ f وحيدة (بدون حساب النوايا المشاركة المتشاكلة) .

١٠-١ الرتبة والدليل Order and Index

١-١٠-١ تعريف : (أ) لتكن X مجموعة . نعرف رتبة (X) كالآتى :

رتبة (X) $(\text{Ord}(X))$ =: { عدد عناصر X إذا كانت X منتهية ؛ ∞ ، إذا كانت X غير منتهية }

(ب) لتكن G زمرة ، ولتكن H زمرة جزئية من G ولتكن G/H مجموعة المجموعات المشاركة اليسرى من G بالنسبة إلى H . يسمى

$$[G:H] := Ord(G/H)$$

دليل H فى G . (The index of H in G)

٢-١٠-١ ملحوظة : لتكن G زمرة ، H زمرة جزئية من G . لكل $a \in G$ الراسم

$$\varphi : H \to aH, \quad h \mapsto ah$$

تناظر أحادى (لأن له الراسم العكسى

$$\varphi^{-1} : aH \to H, \quad ah \mapsto a^{-1}(ah) = h$$
.

ومن ثم فإن : $\forall a \in G: \qquad Ord(ah) = Ord(H)$

٣-١٠-١ نظرية لاجرانج Lagrange's Theorem

لتكن G زمرة منتهية ، H زمرة جزئية من G . عندئذ فإن :

$$Ord(G) = [G:H].Ord(H)$$

البرهان : سنثبت أولاً أن مجموعة المجموعات المشاركة اليسرى بالنسبة إلى H تكون تجزئة (partition) فى G .

واضح- أولاً- أن كل عنصر فى G ينتمى- على الأقل- إلى مجموعة مشاركة يسرى لأن:

$$\forall g \in G: \quad g = ge \in gH \quad (e \text{ العنصر المحايد فى } G)$$

ثانياً : ليكن $gH \cap g'H \ni gh = g'h'$. ينتج أن $g = g'h'h^{-1} \in g'H$ وهذا يقتضى أنه لكل $gh'' = g'h'h^{-1}h'' \in g'H : h'' \in H$ ، وهذا يستلزم أن $gH \subset g'H$. وبالمثل يثبت أن $g'H \subset gH$. ومن ثم فإن $gH = g'H$. أى أن المجموعات المشاركة اليسرى بالنسبة إلى H إما أن يكون تقاطعها خالياً (empty) أو تتطابق ، ومن أولاً ينتج أنها تكون تجزئة لـــ G .

ومن حيث إنه لكل $g \in G$ يكون $Ord(gH) = Ord(H)$ (ملحوظة (١-١٠-٢)) ينتج منطوق النظرية مباشرة .

١-١٠-٤ نتيجة : إذا كان رتبة (Order) الزمرة G عدداً أولياً فإن G لاتحتوى من الزمر الجزئية إلا التافهتين .

البرهان : ليكن رتبة (G) هو العدد الأولى p . من نظرية لاجرانج ينتج أن : $Ord(H)=1$ أو $Ord(H)=p$. $Ord(H)=1$ يقتضى أن $H=\{e\}$. $Ord(H)=p$ يقتضى أن $H=G$.

١-١١ الزمر الدائرية Cyclic Groups

١-١١-١ تعريف : لتكن G زمرة ، $X \subset G$ (مجموعة جزئية) . تسمى المجموعة

$$[X] := \cap\{H : H \hookrightarrow G \quad (\text{زمرة جزئية}) \text{ و } X \subset G\}$$

الزمرة الجزئية فى G المتولدة من X (The subgroup of G generated from X)

لأى $a \in G$ سنكتب $[a]$ بدلاً من $[\{a\}]$.

ونعرف **رتبة العنصر** $a \in G$ كالآتى :

$$Ord(a) := Ord([a]) \quad \text{رتبة } (a)$$

١-١١-٢ تمهيدية : لتكن G زمرة ، $X \subset G$ (مجموعة جزئية). عندئذ فإن :

(١) $[X]$ هى أصغر زمرة جزئية من G تحتوى على X

(٢) $[X] = \{a \in G \mid \exists n \in \mathbb{N} \setminus \{0\}, x_1,\ldots,x_n \in X, \varepsilon_1,\ldots,\varepsilon_n \in \{1,-1\} : a = x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}\}$

أى أن $[X]$ هى مجموعة كل حواصل الضرب المنتهية من عناصر $X \cup \{x^{-1} \mid x \in X\}$.

البرهان : (١) ينتج مباشرة من أن تقاطع مجموعة من الزمر الجزئية من زمرة هو زمرة جزئية من نفس الزمرة (انظر (١-٤-٤) مثال٦) .

(٢) سنسمى المجموعة التى فى الطرف الأيمن من (٢) H

"$\supset$" : من حيث إن $[X]$ زمرة جزئية من G تحتوى على كل عناصر X ، فهى تحتوى على كل حواصل الضرب الممكنة من هذه العناصر ومعكوساتها ، أى أن $[X] \supset H$.

"$\subset$" : H زمرة جزئية من G لأنها تحتوى على كل العناصر x_1 ، ... ، x_n (بأخذ $a = x_1^1$ ، $a = x_2^1$ ، ...) . كذلك لكل $a,b \in H$:

$$ab^{-1} = x_1^{\varepsilon_1}...x_n^{\varepsilon_n}.(y_1^{\delta_1}...y_m^{\delta_m})^{-1}, x_1,...,x_n, y_1,...,y_m \in X, \varepsilon_1,...,\varepsilon_n, \delta_1,...,\delta_m \in \{1,-1\}$$
$$= x_1^{\varepsilon_1}...x_n^{\varepsilon_n} y_m^{-\delta_m}...y_1^{\delta_1} \in X$$

إذن هى زمرة جزئية من G وتحتوى على X . ولكن $[X]$ هى أصغر زمرة جزئية فى G تحتوى على X . أى أن $[X] \subset H$.

<u>**١-١١-٣ تعريف**</u>: لتكن G زمرة لها العنصر المحايد e ، $a \in G$. سنعرف العنصر $a^n \in G$ ، $n \in \mathbb{N}$ استقرائياً (inductively) كالآتى :

$$\left.\begin{aligned} a^o &:= e \\ a^k &:= aa^{k-1} \\ a^{-k} &:= (a^k)^{-1} \end{aligned}\right\}, k \in \mathbb{N} \setminus \{0\}$$

وإذا أشرنا إلى الربط بـــ "+" سنكتب na بدلا من a^n ونكتب التعريف كالآتى :

$$\left.\begin{aligned} 0a &:= 0 \\ ka &:= a + (k-1)a \\ (-k)a &:= -(ka) \end{aligned}\right\}, k \in \mathbb{N} \setminus \{0\}$$

<u>**١-١١-٤ قواعد الحساب**</u>: باستخدام الاستقراء الرياضى يمكن البرهنة بسهولة على أن :

(١) لجميع $a \in G$ (G زمرة) ولجميع $m,n \in \mathbb{Z}$:

$$a^m a^n = a^{m+n}, (a^m)^n = a^{mn}$$

(٢) فى زمرة G، $a,b \in G$ إذا كان $ab = ba$ فإنه لجميع $n \in \mathbb{Z}$:

$$(ab)^n = a^n b^n$$

<u>**١-١١-٥ ملحوظة**</u> : ليكن زمرة $a \in G$. ينتج مباشرة من (١-١١-٢) أن :

$$[a] = \{a^n \mid n \in \mathbb{Z}\}$$

<u>**١-١١-٦ تعريف**</u> : يقال لزمرة G إنها <u>**دائرية**</u> (Cyclic) إذا وجد عنصر $a \in G$ بحيث يكون $G = [a]$. ويسمى a فى هذه الحالة <u>**مولداً**</u> (Generator) لـــ G .

<u>**١-١١-٧ نظرية**</u> : (١) كل زمرة دائرية تكون إبدالية .

(٢) إذا كان رتبة زمرة ما عدداً أولياً كانت الزمرة دائرية .

(٣) إذا كانت G زمرة دائرية ، وكان a مولداً لها فإن الراسم

$$\varphi: \mathbb{Z} \to G$$
$$n \mapsto a^n$$

إبيمورفيزم

(٤) كل زمرة جزئيةً من زمرة دائرية تكون دائرية .

البرهان : (١) لتكن G زمرة دائرية وليكن $a,b \in G$. إذن يوجد $m,n \in \mathbb{Z}$ بحيث يكون $a = x^m$ ، $b = x^n$ حيث x مولد للزمرة G .

وهذا يقتضى أن :

$$ab = x^m x^n = x^{m+n} = x^{n+m} = x^n x^m = ba$$

١-١١-٤

أى أن G إبدالية .

(٢) ليكن $e \in G$ العنصر المحايد فى الزمرة G. رتبة (G) عدد أولى (1 ليس عدداً أولياً) يستلزم أنه يوجد عنصر $e \neq a \in G$ ومن ثم فإن $[a] \neq \{e\}$ زمرة جزئية فى G. ومن (١-١٠-٤) ينتج أن $[a] = G$ ، أى أن G دائرية .

(٣) واضح أن φ راسم فوقى (شامل). φ هومومورفيزم لأن :

$$\forall m,n \in \mathbb{Z}: \ \varphi(m+n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n)$$

١-١١-٤

أى أن φ إبيمورفيزم .

(٤) لتكن G زمرة دائرية ، H زمرة جزئية من G، a مولد لـــ G . من (٣)

$\varphi: \mathbb{Z} \to G$، $n \mapsto a^n$ إبيمورفيزم وبالتالى فإن $\varphi^{-1}(H)$ زمرة جزئية من $\mathbb{Z}$(راجع ١-٤-٣

(ب)) ومن مثال٣ فى (١-٤-٤) يكون $\varphi^{-1}(H) = m\mathbb{Z}$ حيث $m \in \mathbb{Z}$ ومن حيث إن φ راسم فوقى (شامل) يكون :

$$H = \varphi(\varphi^{-1}(H)) = \varphi(m\mathbb{Z})$$
$$= \{(a^m)^n (= a^{mn}) \mid n \in \mathbb{Z}\} \qquad (a^m \text{ مولد } H)$$

١-١١-٨ نظرية تفصيل الزمر الدائرية — Classification of cyclic groups

لتكن G زمرة دائرية ، a مولد لـــ G، $m := Ord(G)$. عندئذ فإن :

(١) إذا كانت $m=\infty$ فإن الراسم $\begin{matrix}\varphi:\mathbb{Z}\to G\\ n\mapsto a^n\end{matrix}$ أيزومورفيزم .

(٢) إذا كانت $m<\infty$ فإن الراسم $\begin{matrix}\varphi:\mathbb{Z}/m\mathbb{Z}\to G\\ n+m\mathbb{Z}\mapsto a^n\end{matrix}$ لجميع $n\in\mathbb{Z}$ أيزومورفيزم .

البرهان : $\begin{matrix}\varphi:\mathbb{Z}\to G\\ n\mapsto a^n\end{matrix}$ إبيمورفيزم من (١-١١-٧) (٣) .

والآن نطبق نظرية الهومومورفيزم (١-٨-١)

$$\varphi(\mathbb{Z})\cong \mathbb{Z}/Ker(\varphi)$$

ولأن φ راسم فوقى يكون $\varphi(\mathbb{Z})=G$ ومن ثم فإن $G\cong \mathbb{Z}/Ker(\varphi)$.

إذا كان $Ord(G)=m<\infty$ فإن $Ker(\varphi)\neq\{0\}$ وإلا كان $G\cong \mathbb{Z}/\{0\}\cong\mathbb{Z}$ وتكون $\mathbb{Z}$ منتهية

وهذا تناقض وبالتالى فإن $Ker(\varphi)=n\mathbb{Z},n\in\mathbb{Z}$ ويكون $m=Ord(G)=Ord(\mathbb{Z}/n\mathbb{Z})=n$

$\Leftarrow$ $G\cong\mathbb{Z}/m\mathbb{Z}$ ويكون $\begin{matrix}\psi:\mathbb{Z}/m\mathbb{Z}\to G\\ n+m\mathbb{Z}\mapsto a^n\end{matrix}$ هو الأيزومورفيزم الموجود .

أما إذا كان $Ord(G)=\infty$ فإن φ يكون راسماً واحداً لواحد (injective) لأنه بفرض أن

$$\varphi(m)=a^m=a^n=\varphi(n)\quad,\quad m,n\in\mathbb{Z},m>n$$

فإنه ينتج أن e) العنصر المحايد فى G) $a^{m-n}=e$ ، $m-n>0$. وليكن k هو أصغر عدد صحيح موجب بحيث إن $a^k=e$. نحن ندعى أن G تتكون بالضبط من العناصر e، a، a^2، ...، a^{k-1} . ليكن $a^\ell\in G$، عندئذ فإنه يوجد عددان صحيحان r,q بحيث إن :

$$\ell=kq+r\quad,\quad 0\le r<k$$

ويكون

$$a^\ell=a^{kq+r}=(a^k)^q a^r=e^q a^r=a^r,0\le r<k$$

وهذا يعنى أن G منتهية : تناقض .

والآن φ راسم واحد لواحد $\Leftarrow$ $Ker(\varphi)=\{0\}$ $\Leftarrow$

١-٣-٥

$$G=\varphi(\mathbb{Z})\cong\mathbb{Z}/\{0\}\cong\mathbb{Z}$$

ويكون
$$\varphi:\mathbb{Z}\to G$$
$$n\mapsto a^n$$
هو الأيزومورفيزم الموجود .

١-١١-٩ نتيجة : لتكن G زمرة ، e عنصرها المحايد

(١) لكل $a\in G$ لكل $k\in\mathbb{Z}$: $a^k=e \Leftrightarrow$ رتبة (a) $(Ord(a))$ تقسم k .

(٢) لكل $a\in G$: $a^{Ord(G)}=e$ (نظرية كلاين – فرمات) .

البرهان : (١) ليكن $Ord(a)=m$ ، $\psi:\mathbb{Z}/m\mathbb{Z}\to[a]$, $k+m\mathbb{Z}\mapsto a^k$ الأيزومورفيزم الذى حصلنا عليه فى (١-١١-٨) . عندئذ فإن :
$$a^k=e\Leftrightarrow k+m\mathbb{Z}\in Ker(\psi)=m\mathbb{Z}$$
$$\Leftrightarrow k\in m\mathbb{Z}\Leftrightarrow \exists \ell\in\mathbb{Z}:k=m\ell$$
أى أن m تقسم k .

(٢) ليكن $a\in G$. من (١) : $a^{Ord(a)}=e$. من نظرية لاجرانج (١-١٠-٣) رتبة (a) $(Ord(a))$ تقسم $Ord\ (G)$ أى أنه يوجد $k\in\mathbb{Z}$ بحيث يكون : $Ord(G)=k.Ord(a)$.
وبالتالى فإن:
$$a^{Ord(G)}=a^{k\cdot Ord(a)}=(a^{Ord(a)})^k=e^k=e$$

١-١١-١٠ نتيجة : لتكن G زمرة ، $a\in G$, $Ord(a)=m<\infty$. عندئذ فإن
$$[a]=\{a^k:k\in\{0,\dots,m-1\}\}$$

البرهان : من (١-١١-٨) يوجد أيزومورفيزم
$$\psi:\mathbb{Z}/m\mathbb{Z}\to[a] \qquad \forall k\in\mathbb{Z}$$
$$k+m\mathbb{Z}\mapsto a^k$$
ومن ثم فإن :
$$[a]=\psi(\mathbb{Z}/m\mathbb{Z})=\{\psi(k+m\mathbb{Z}):k\in\{0,\dots,m-1\}\}$$

١-١١-١١ استنتاج : لتكن G زمرة دائرية منتهية لها الرتبة $m\geq 2$ ، a مولد لـ G، $b\in G$. عندئذ فإن b يكون مولداً لـ G إذا وجد وفقط إذا وجد عدد طبيعى r ليس بينه وبين m قواسم مشتركة (عدا ±1 بالطبع) بحيث يكون $b=a^r$.

البرهان : " $\Rightarrow$ " : ليكن r عدداً طبيعياً ليس بينه وبين m قواسم مشتركة ، بحيث إن $b=a^r$. لأن r، m ليس بينهما قواسم مشتركة فإنه من نظرية الأعداد الابتدائية (Elementary Number Theory) يوجد $k,\ell\in\mathbb{Z}$ بحيث يكون: $km+\ell r=1$ وينتج أن:

$$a=a^{km+\ell r}=(a^m)^k(a^r)^\ell=e^k(a^r)^\ell=e(a^r)^\ell=(a^r)^\ell=b^\ell$$

ومن ثم فإن : $G=[a]\subset[b]\subset G$

$$\Rightarrow \quad G=[b]$$

" $\Leftarrow$ " : لأن a مولد لـG فمن (١-١١-١٠) يوجد $r\in\mathbb{N}$ بحيث يكون $b=a^r$.

ليكن $t\in\mathbb{Z}$ قاسماً مشتركاً بين m، r . عندئذ فإنه يوجد $k,\ell\in\mathbb{Z}$ بحيث يكون $m=kt$، $r=\ell t$. إذا كان b مولداً لـ G فإنه ينتج أن :

(e العنصر المحايد فى G)

$$b^k=a^{rk}=a^{\ell tk}=(a^m)^\ell=e^\ell=e, |k|\geq m$$

(من (١-١١-٩) ولأن b مولد لـ G فرتبته = رتبة $(G)=m$) . ومع $m=kt$ ينتج أن $|t|=1$.

<u>١-١١-١٢ **استنتاج**</u> : لتكن G زمرة دائرية منتهية لها الرتبة m . عندئذ فإنه لكل t قاسم موجب لـ m يوجد بالضبط زمرة جزئية واحدة من G لها الرتبة t .

البرهان : ليكن e عنصر G المحايد ، وليكن a مولداً لـ G و $k\in\mathbb{N}$ بحيث إن $m=tk$.

نبرهن أولاً على أن الزمرة الجزئية $H:=[a^k]$ من G لها الرتبة t ، وذلك كالآتى : لأن $(a^k)^t=a^m=e$ فإن (1) $Ord(H)\leq t$. ومن $a^{k.Ord(H)}=(a^k)^{Ord(H)}=e$ ينتج أن :

$$k.Ord(H)\geq Ord(a)=Ord(G)=kt$$

وبالتالى فإن (2) $Ord(H)\geq t$. من (1) ، (2) ينتج المطلوب

ثانيا : لتكن H' زمرة جزئية من G لها الرتبة t ، فمن (١-١١-٧) (٤) يوجد $\ell\in\mathbb{N}$ بحيث إن $H'=[a^\ell]$. ومما سبق ينتج أن :

$$\frac{m}{k}=t=Ord(H')=\frac{m}{\ell}$$

وبالتالى فإن $\ell=k$ ويكون $H=H'$.

١-١١-١٣ نتيجة : لتكن G زمرة ، e عنصرها المحايد. وليكن $G \neq \{e\}$ ، G ، $\{e\}$ الزمرتين الجزئيتين الوحيدتين فى G. عندئذ فإنه يوجد عدد أولى p بحيث إن $G \cong \mathbb{Z}/p\mathbb{Z}$.

(من نظرية لاجرانج لأى عدد أولى p تحتوى الزمرة $\mathbb{Z}/p\mathbb{Z}$ الزمرتين الجزئيتين التافهتين فقط)

البرهان : لأن G لاتحتوى من الزمر الجزئية إلا التافهة فقط فإنه لأى : $e \neq a \in G$ يكون $[a] = G$. وبالتالى فإن G تكون دائرية . ومن (١-١١-٨) فإنه يوجد $n \in \mathbb{N}$ بحيث إن : $G \cong \mathbb{Z}/n\mathbb{Z}$. إذا كان n عدداً ليس أولياً فإنه من (١-١١-١٢) توجد زمر جزئية غير تافهة من $\mathbb{Z}/n\mathbb{Z}$ أى من G وهذا تناقض مع كونها لاتحتوى من الزمر الجزئية إلا على التافهة .

أمثلة متنوعة

مثال ١: لتكن G زمرة بحيث إنه لكل $a \in G$: $a^2 = e$ (e العنصر المحايد فى G) .
برهن على أن G إبدالية .

البرهان : $\forall a, b \in G$

$$ba = ebae = (aa)ba(bb) = a(ab)(ab)b = aeb = ab$$

طريقة أخرى :

$$a^2 = e, b^2 = e, (ab)^2 = e \Rightarrow a = a^{-1}, b = b^{-1}, ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

طريقة ثالثة :

$$e = (ab)(ab) = a^2b^2 = aabb \Rightarrow ba = a^{-1}ababb^{-1} = a^{-1}aabbb^{-1} = ab$$

مثال ٢ : برهن على أن أية زمرة مكونة من أربعة عناصر مختلفة تكون إبدالية .

البرهان: لتكن G زمرة مكونة من الأربعة عناصر المختلفة x ، y ، z ، e حيث e عنصرها المحايد. ولتكن G غير إبدالية. عندئذ فإنه يوجد من عناصرها عنصران x ، y ، بدون فقد للعمومية ، بحيث يكون $e = xy \neq yx = z$
(الإمكانية $x = yx$ مستبعدة وإلا : $y = y(xx^{-1}) = (yx)x^{-1} = xx^{-1} = e$ وكذلك الإمكانات $yx = y, xy = x, xy = y$ كلها مستبعدة) .
والآن : $xy = e \Rightarrow x = y^{-1} \underset{yx=z}{\Rightarrow} z = yx = yy^{-1} = e$
تناقض مع $z \neq e$.

طريقة أخرى: إذا كانت G دائرية فإنها تكون إبدالية حسب (١-٧-١١) (١). لتكن G غير دائرية . فمن نظرية لاجرانج رتبة أى عنصر فى زمرة يكون قاسماً لرتبة الزمرة . وبالتالى فإن العناصر x ، y ، z لها فقط الرتبة ٢. (الرتبة ٤ مستبعدة لأى منها وإلا أصبحت الزمرة دائرية. الرتبة ١ تعنى أن العنصر هو e) ، أى أن $x^2 = y^2 = z^2 = e$.
من مثال١ ينتج المطلوب مباشرة .

طريقة ثالثة : إما أن الزمرة تحتوى على زمر جزئية غير تافهة وإما أنها تحتوى من الزمر الجزئية على التافهة فقط. فى الحالة الأخيرة وفقاً للبرهان فى (١-١١-١٣) تكون الزمرة دائرية ومن ثم تكون إبدالية .

فى الحالة الأولى : تكون الزمر الجزئية لها رتبة تقسم رتبة الزمرة٤ . أى لها الرتبة ٢ .
لدينا الآن الإمكانات الآتية :

(أ) توجد ثلاث زمر جزئية ، أى أن : $x^2 = y^2 = z^2 = e$

وكما سبق تكون الزمرة إبدالية .

(ب) توجد زمرتان جزئيتان ، وبدون فقد للعمومية يكون : $x^2 = y^2 = e$ ، $z^2 \neq e$.

وبالتالى لايكون هناك معكوس لـــ z : تناقض مع كون G زمرة .

(جــ) توجد زمرة جزئية واحدة ، وبدون فقد للعمومية يكون: $x^2 = e$ ، $y^2 \neq e \neq z^2$.

يكون لدينا بالضرورة "الضرب" الآتى :

$$yz = e = zy$$

$$xy = z = yx$$

$$xz = y = zx$$

أى أن الزمرة إبدالية .

مثال ٣ : لتكن $(G, \cdot_G)$ زمرة (ربطها هو $\cdot_G$) ، ولتكن $H \subset G$ (مجموعة جزئية) .
وليكن $\iota := (H, G, \{(a,a) \mid a \in H\})$ هو راسم التضمين (The inclusion mapping) .
إذا وجد ربط $\cdot_H$ على H بحيث يكون $(H, \cdot_H)$ زمرة ، ι هومومورفيزم تسمى عندئذ **H زمرة جزئية من G** . ونكتب $H \hookrightarrow G$. (سنبرهن فى مثال٤ على أن هذا التعريف متسق مع التعريف المعروف الموجود فى (١-٤-١)) .

برهن على أن الربط $\cdot_H$ وحيد وأن $\forall a,b \in H: \ a \cdot_H b = a \cdot_G b$.

البرهان :

$$\forall a,b \in H : a \cdot_H b = \iota(a \cdot_H b) \underset{\iota \text{ هومومورفيزم}}{=} \iota(a) \cdot_G \iota(b) = a \cdot_G b$$

مثال ٤ : لتكن $\phi \neq U \subset G$ مجموعة جزئية غير خالية . التقريرات الآتية متكافئة :

(1) $U \hookrightarrow G$ (U زمرة جزئية من G) بالمفهوم فى مثال ٣ السابق .

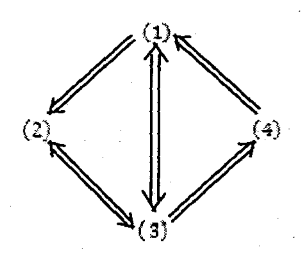
(2) لكل $x, y \in U$: $xy^{-1} \in U$ (U زمرة جزئية بالمفهوم (١-٤-١) من التمهيدية (١-٤-٢)).

(3) لكل $x \in U$: $x^{-1} \in U$ ، ولكل $x, y \in U$: $xy \in U$

وإذا كانت U **منتهية** (finite) يكون أى تقرير من التقارير السابقة مكافئاً لـــ :

(4) لكل $x, y \in U$: $xy \in U$

البرهان : سنجرى البرهان بإظهار الاقتضاءات (الاستلزامات) الآتية :



"$(2) \Rightarrow (1)$" ، "$(1) \Rightarrow (3)$" : واضحان من مثال ٣ .

"$(2) \Rightarrow (3)$" ، "$(4) \Rightarrow (3)$" : تافهان ! (trivial) .

"$(1) \Rightarrow (4)$" : الراسم $\begin{matrix} \varphi : U \to U \\ y \mapsto xy \end{matrix}$ $\forall x \in U$

راسم واحد لواحد ، ولأن U منتهية إذن هو تناظر أحادى . وبالمثل فإن

$\begin{matrix} \psi : U \to U \\ x \mapsto xy \end{matrix}$ $\forall y \in U$

هو تناظر أحادى كذلك . ولأن الربط : $U \times U \ni (x, y) \mapsto xy \in U$ إدماجى (تشاركى ، تجميعى) فينتج مباشرة من (١-٢-٦) أن U زمرة .

والآن $\iota(xy) = xy = \iota(x)\iota(y)$

(تذكر أن $(\cdot_U = \cdot_G)$

فينتج أن $G \hookleftarrow U$ (بالمفهوم فى مثال ٣) .

"$(1) \Rightarrow (3)$" : لأن $U \neq \phi$ فإنه يوجد $x \in U$ ومن (3) يوجد $x^{-1} \in U$ ومن (3) كذلك $xx^{-1} = e \in U$. الربط $U \times U \ni (x, y) \mapsto xy \in U$ تشاركى (إدماجى) فينتج أن U زمرة. كذلك كما سبق $\iota(xy) = xy = \iota(x)\iota(y)$.

ينتج أن $G \hookleftarrow U$ (بالمفهوم فى مثال ٣) .

"$(2) \Rightarrow (3)$" : $x \in U \Rightarrow x, x \in U \underset{(2)}{\Rightarrow} e = xx^{-1} \in U$

$$e,x\in U \underset{(2)}{\Rightarrow} ex^{-1}=x^{-1}\in U \qquad (*)$$

$$x,y\in U \underset{(*)}{\Rightarrow} x,y^{-1}\in U \underset{(2)}{\Rightarrow} x(y^{-1})^{-1}=xy\in U.$$

<u>**مثال ٥**</u> : برهن على أن الزمرة $(\mathbb{Q},+)$ ليست دائرية .

<u>**البرهان**</u> : لتكن $(\mathbb{Q},+)$ دائرية. إذن يوجد مولد $\frac{m}{n}\in\mathbb{Q}$ حيث $m,n\in\mathbb{Z}$ ، $n\neq 0$ ، بحيث إنه لأى $q\in\mathbb{Q}$ يوجد $k\in\mathbb{Z}$ بحيث إن $q=k.\frac{m}{n}$. والآن :

$$\mathbb{Q}\ni\frac{1}{2n}=\ell.\frac{m}{n},\ \ell\in\mathbb{Z}\Rightarrow 1=2m\ell,\ \ m,\ell\in\mathbb{Z}$$ تناقض

إذن $(\mathbb{Q},+)$ ليست دائرية .

<u>**مثال ٦**</u> : لتكن $H\subset G$ زمرة جزئية طبيعية (من G)، $K\subset G$ زمرة جزئية بحيث إن :

$$H\subset K\subset G$$

برهن على أن $H\subset K$ زمرة جزئية طبيعية .

<u>**البرهان**</u> : واضح أن H زمرة جزئية من K . والآن :

$$\forall k\in K \quad \forall h\in H: \quad khk^{-1}\in H$$

(لأن $k\in K\Rightarrow k\in G$ ، H زمرة جزئية طبيعية فى G) .

H زمرة جزئية طبيعية فى K $\Rightarrow$.

<u>**مثال ٧**</u> : لتكن G زمرة ، $H\subset G$ زمرة جزئية طبيعية ، $L\subset G$ زمرة جزئية .

برهن على أن : $H\cap L\subset L$ زمرة جزئية طبيعية (من L) .

<u>**البرهان**</u> : نلاحظ أولاً أن $H\cap L\subset L$ زمرة جزئية (من L) لأن :

(e هو العنصر المحايد فى G) $\qquad e\in L, e\in H\Rightarrow H\cap L\neq\phi$

$$\forall a,b\in H\cap L: ab^{-1}\in H, ab^{-1}\in L\Rightarrow ab^{-1}\in H\cap L$$

أى أن $H\cap L$ زمرة جزئية من L .

والآن :

$$\forall x\in H\cap L \quad \forall \ell\in L: \ell x\ell^{-1}\in L,\ \ell x\ell^{-1}\in H$$

(لأن $\ell\in L\Rightarrow\ell\in G$ ، $H\subset G$ زمرة جزئية طبيعية) .

$$\Rightarrow \forall \ell \in L \ \ \forall x \in H \cap L : \ell x \ell^{-1} \in H \cap L$$

أى أن $H \cap L$ زمرة جزئية طبيعية فى L .

مثال ٨ : اختبر إذا ما كان هناك أيزومورفيزم بين الزمر الآتية :

(١) (γ_4, o) (الزمرة المتماثلة على أربعة عناصر) ، $(\mathbb{Z}/4\mathbb{Z}, +)$.

(٢) $(\mathbb{Z}, +)$ ، $(5\mathbb{Z}, +)$

(٣) $(\mathbb{Z}, +)$ ، $(\mathbb{Q}, +)$

(٤) $(\mathbb{R} \setminus \{0\}, .)$ ، $(\mathbb{C} \setminus \{0\}, .)$

(٥) زمرتان منتهيتان لهما نفس الرتبة إحداهما دائرية والأخرى ليست دائرية .

الحل : (١) لايوجد أيزومورفيزم لأن رتبة (γ_4, o) هى: $4! = 24$ بينما رتبة $(\mathbb{Z}/4\mathbb{Z}, +)$: 4

ولايمكن أن يوجد تناظر أحادى بين مجموعتين منتهيتين تختلفان فى الرتبة .

لاحظ كذلك أن $(\mathbb{Z}/4\mathbb{Z}, +)$ إبدالية بينما $(\gamma_4, 0)$ ليست إبدالية (انظر مثال٣ بند (١-٢-٥))

ولايمكن أن يوجد أيزومورفيزم بين زمرتين إحداهما إبدالية والأخرى ليست ابدالية (انظر مثال ٩ بند (١-٣-٨)) .

(٢) يوجد أيزومورفيزم بين $(\mathbb{Z}, +)$ ، $(5\mathbb{Z}, +)$

يعطى كالآتى :

$$\varphi : \mathbb{Z} \to 5\mathbb{Z}$$
$$z \mapsto 5z$$

φ تناظر أحادى لأنه يوجد الراسم العكسى

$$\psi : 5\mathbb{Z} \to \mathbb{Z}$$
$$5z \mapsto z$$

حيث

$$\psi o \varphi : \mathbb{Z} \to \mathbb{Z} \quad , \quad \varphi o \psi : 5\mathbb{Z} \to 5\mathbb{Z}$$
$$z \mapsto z \qquad\qquad 5z \mapsto 5z$$

أى أن $\psi o \varphi = 1_{\mathbb{Z}}$ ، $\varphi o \psi = 1_{5\mathbb{Z}}$.

كذلك φ هومومورفيزم لأن :

$$\forall z_1, z_2 \in \mathbb{Z} : \varphi(z_1 + z_2) = 5(z_1 + z_2) = 5z_1 + 5z_2 = \varphi(z_1) + \varphi(z_2)$$

إذن φ أيزومورفيزم .

(٣) لايوجد أيزومورفيزم بين $(\mathbb{Z},+)$، $(\mathbb{Q},+)$ لأن $(\mathbb{Z},+)$ دائرية لهـا مولـد"1" ، بينمـا $(\mathbb{Q},+)$ ليست دائرية (مثال٥) ، ونثبت فى الجزء (٥) من هذا المثال أنـه لايمكـن أن يوجد أيزومورفيزم بين أى زمرتين إحداهما دائرية والأخرى ليست دائرية .

لاحظ كذلك أنه فى مثال ١٠ بند (١-٣-٨) برهنا على أنه لايمكن أن يوجد إبيمـورفيزم من $(\mathbb{Q},+)$ على $(\mathbb{Z},+)$ وبالتالى فلا يمكن أن يوجد أيزومورفيزم بينهما .

(٤) لايوجد أيزومورفيزم بين $(\mathbb{R}\setminus\{0\},.)$ ، $(\mathbb{C}\setminus\{0\},.)$.

كل عنصر فى $\mathbb{R}\setminus\{0\}$ يولد زمرة جزئية دائرية غير منتهية فيما عـدا 1 ، 1- . 1 يولد الزمرة الجزئية $\{1\}$ لها الرتبة 1 ، بينما 1- يولد الزمرة$\{1- ، 1\}$ لها الرتبة 2 . أما فى $\mathbb{C}\setminus\{0\}$ فإن العنصر i يولد الزمرة الجزئية الدائرية $\{i,1,-i,-1\}$ لها الرتبة 4 .

(٥) لايوجد أيزومورفيزم . البرهان بالتناقض .

لتكن G زمرة دائرية لها المولد a، G' زمرة غير دائرية وليكن

$$\varphi : G \to G'$$
$$a \mapsto a'$$

أيزومورفيزم .

ليكن $x' \in G'$. لأن φ تناظر أحادى فإنه يوجد واحـد بالـضبط $x \in G$ بحيـث إن $x' = \varphi(x)$.

$$x \in G \quad \Rightarrow \quad \exists m \in \mathbb{Z} : x = a^m$$

دائرية G

$$x' = \varphi(a^m) \quad = \quad \varphi(a)^m := (a')^m$$

φ هومومورفيزم

أى أن $a' := \varphi(a)$ مولد لـG' وتكون G' دائرية : تناقض .

مثال ٩ : فى γ_3 (الزمرة المتماثلة على ثلاثة عناصر) اوجد :

(١) جميع الزمر الجزئية .

(٢) كل المجموعات المشاركة اليسرى بالنسبة إلى $\{e,(23)\}$ حيث e هو العنـصر المحايد فى γ_3.

(٣) كل الزمر الجزئية الطبيعية غير التافهة .

(٤) كل زمر القسمة الناشئة من (٣)

(٥) المطبع (The normalizer) لـ $\{e,(12)\}$

الحل : جدول الضرب فى γ_3 موضح كالآتى

	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_2	e	σ_5	σ_3	σ_4
σ_2	σ_2	e	σ_1	σ_4	σ_5	σ_3
σ_3	σ_3	σ_4	σ_5	e	σ_1	σ_2
σ_4	σ_4	σ_5	σ_3	σ_2	e	σ_1
σ_5	σ_5	σ_3	σ_4	σ_1	σ_2	e

حيث e هو العنصر المحايد ، $\sigma_1=(1\ 2\ 3)$ ، $\sigma_2=(1\ 3\ 2)$ ، $\sigma_3=(2\ 3)$ ، $\sigma_4=(1\ 3)$ ، $\sigma_5=(1\ 2)$.

$(1\ 2\ 3)$ تعنى $1\to 2$ ، $2\to 3$ ، $3\to 1$

طريقة حساب الجدول : على سبيل المثال لإيجاد $\sigma_3\,\sigma_2$ نأخذ σ_2 من العمود الثالث و σ_3 من الصف الرابع ونجرى حاصل الضرب بهذا الترتيب فنحصل على σ_5 . ولاحظ أننا هنا استخدمنا التعريف الذى فضلناه كما أشرنا فى نهاية مثال ٣ من بند (١-٢-٥) .

(١) من نظرية لاجرانج رتبة الزمرة الجزئية من زمرة تقسم رتبة الزمرة . ولأن رتبة (γ_3) هى $3!=6$ فإن الزمر الجزئية فى γ_3 لها الرتب :

1 وتكون الزمرة الجزئية هى $\{e\}$

2 وتكون هناك ثلاث زمر جزئية هى $\{e,(1\ 2)\}, \{e,(1\ 3)\}, \{e,(2\ 3)\}$

3 وتكون الزمرة الجزئية الوحيدة هى $\{e,(1\ 2\ 3),(1\ 3\ 2)\}$

6 وتكون هى γ_3

(٢)
$$e\{e,(2\ 3)\} = \{e,(2\ 3)\}$$
$$(1\,2)\{e,(2\ 3)\} = \{(1\,2),(1\ 2\ 3)\}$$
$$(1\,3)\{e,(2\ 3)\} = \{(1\,3),(1\ 3\ 2)\}$$

$$(2\ 3)\{e,(2\ \ 3)\} = \{e,(2\ 3)\}$$

$$(1\ 2\ \ 3)\{e,(2\ \ 3)\} = \{(1\ 2),(1\ \ 2\ \ 3)\}$$

$$(1\ 3\ \ 2)\{e,(2\ \ 3)\} = \{(1\ 3),(1\ \ 3\ \ 2)\}$$

(٣) اختبر : $\forall a \in G: \quad aNa^{-1} = N \quad (G = \gamma_3)$

الزمرة الجزئية الطبيعية الوحيدة غير التافهة هي $\{e,(1\ \ 2\ \ 3),(1\ \ 3\ \ 2)\}(=N)$

(بالإضافة إلى الزمرتين الجزئيتين التافهتين γ_3 ، $\{e\}$)

(٤) توجد زمرة جزئية طبيعية وحيدة (غير تافهة) N هى $N=\{e,(1\ 2\ 3),(1\ 3\ 2)\}$

وتكون لدينا زمرة القسمة γ_3/N التى عناصرها هى :

$eN,(1\ \ 2\ \ 3)N,\ (1\ \ 3\ \ 2)N,\ (1\ \ 2)N,\ (1\ \ 3)N,\ (2\ \ 3)N$

ولكن $eN = (1\ \ 2\ \ 3)N = (1\ \ 3\ \ 2)N = N$

لأن $e,\ (1\ \ 2\ \ 3),(1\ \ 3\ \ 2) \in N$

أما $(1\ \ 2)N = (1\ \ 3)N = (2\ \ 3)N = \{(1\ \ 2),(1\ \ 3),(2\ \ 3)\}$

وبالتالى تتكون γ_3/N من عنصرين فقط هما: $N,\{(1\ 2),(1\ 3),(2\ 3)\}$ ولاحظ أن هذا يتفق مع نظرية لاجرانج حيث إن عدد عناصر γ_3 هو 6 ، عدد عناصر N هو 3 وبالتالى يكون عدد عناصر γ_3/N هو 2 . ولاحظ أن $N \cap \{(1\ \ 2),\ (1\ \ 3),\ (2\ \ 3)\} = \phi$ كما نعلم ذلك من برهان نظرية لاجرانج .

(٥) لإيجاد مطبع $\{e,(1\ \ 2)\}$ نبحث عن $a \in \gamma_3$ بحيث يكون

$$a\{e,(1\ \ 2)\} = \{e,(1\ \ 2)\}a$$

والحلول هى $a = e, a = (1\ \ 2)$

أى أن $Nor(\{e,(1\ \ 2)\}) = \{e,(1\ \ 2)\}$

<u>**مثال ١٠**</u> : لتكن θ هومومورفيزماً من $(\mathbb{Z},+)$ إلى $(\mathbb{Q}\setminus\{0\},.)$ معرفاً كالآتى :

$$\theta(x) = \begin{cases} 1\ , & x \ \text{عدد زوجى} \\ -1\ , & x \ \text{عدد فردى} \end{cases}$$

اوجد نواة (θ) $(Ker(\theta))$ وحقق نظرية الهومومورفيزم

<u>الحـل</u> : $Ker(\theta)=\{x\in\mathbb{Z}:\theta(x)=1\}$

$=\{x\in\mathbb{Z}:$ عدد زوجي $x\}=2\mathbb{Z}$

ويكون $\mathbb{Z}/Ker(\theta)=\mathbb{Z}/2\mathbb{Z}$ ، بينما $\theta(\mathbb{Z})=\{1,-1\}$

وواضح أن $(\mathbb{Z}/2\mathbb{Z},+)\cong(\{1,-1\},.)$

حيث -1 هو مولد $(\{1،-1\}،.)$ بينما $\bar{1}:=1+2\mathbb{Z}$ هو مولد $(\mathbb{Z}/2\mathbb{Z}+)$. وهو مـــايحقق نظرية الهومومورفيزم .

توضيح : $(-1)\ .\ (-1)\ =\ 1$ ، بينما

$$\bar{1}+\bar{1}=1+2\mathbb{Z}+1+2\mathbb{Z}$$
$$=2+2\mathbb{Z}=2\mathbb{Z}=\bar{0}$$

والأيزومورفيزم يتم هكذا : $\begin{matrix}\bar{0}\leftrightarrow 1\\ \bar{1}\leftrightarrow -1\end{matrix}$.

<u>مثال ١١</u> : حقق أن θ فى المثال السابق مباشرة هومومورفيزم .

<u>الحـل</u> :

$$\forall z_1,z_2\in\mathbb{Z}:\theta(2z_1+2z_2)=\theta(2(z_1+z_2))=1$$
$$=1.1=\theta(2z_1).\theta(2z_2)$$
$$\theta(2z_1+(2z_2+1))=\theta(2(z_1+z_2)+1)=-1$$
$$=1.(-1)=\theta(2z_1).\theta(2z_2+1)$$
$$\theta(2z_1+1+2z_2+1)=\theta(2(z_1+z_2+1))=1$$
$$=(-1).(-1)=\theta(2z_1+1).\theta(2z_2+1)$$

<u>مثال ١٢</u> : ليكن

$$\theta:(\mathbb{Q}\setminus\{0\},.)\to(\mathbb{Q}\setminus\{0\},.)$$
$$x\mapsto|x|$$

حقق أن θ هومومورفيزم وحقق نظرية الهومومورفيزم .

<u>الحـل</u> : $\forall x,y\in\mathbb{Q}\setminus\{0\}:\theta(xy)=|xy|=|x||y|=\theta(x).\theta(y)$

أى أن θ هومومورفيزم

$$Ker(\theta)=\{x:x\in\mathbb{Q}\setminus\{0\},\varphi(x)=1\}$$
$$=\{1,-1\}$$
$$\theta(\mathbb{Q}\setminus\{0\})=\{x:x\in\mathbb{Q},x>0\}=:\mathbb{Q}^*$$

سنبرهن على أن $\left({(\mathbb{Q}/\{0\})}/{\{1,-1\}},.\right) \cong (\mathbb{Q}^{+},.)$ مباشرة ، دون الاستعانة بنظرية الهومومورفيزم :

سنعرف :
$$\varphi : {(\mathbb{Q}/\{0\})}/{\{1,-1\}} \to \mathbb{Q}^{+}$$
$$q\{1,-1\} \mapsto |q|$$

واضح أن φ معرف جيداً (well-defined) .

φ هومومورفيزم لأن :
$$\forall q_1,q_2 \in \mathbb{Q}/\{0\} : \varphi((q_1\{1,-1\}).(q_2\{1,-1\})) = \varphi(q_1q_2\{1,-1\})$$
$$= |q_1q_2| = |q_1||q_2| = \varphi(q_1\{1,-1\}).\varphi(q_2\{1,-1\})$$

φ غامر (شامل) : واضح

φ واحِد لواحد .
$$|q_1| = \varphi(q_1\{1,-1\}) = \varphi(q_2\{1,-1\}) = |q_2| \Rightarrow q_1 = \pm q_2$$
$$\Rightarrow q_1\{1,-1\} = q_2\{1,-1\}$$

أى أن φ أيزومورفيزم . وهذا يتسق مع نظرية الهومومورفيزم للزمر .

<u>مثال ١٣</u> : لتكن G "زمرة" الرواسم من $\mathbb{R}$ على $\mathbb{R}$ (onto) التى على الشكل :
$$\alpha_{a,b} : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto ax+b, \qquad a \neq 0, a,b,x \in \mathbb{R}$$

برهن على ان الراسم : $\theta : G \to G$ ، $\alpha_{a.b} \mapsto \alpha_{a,0}$ هومومورفيزم من G إلى G . اوجد نواة (θ) وصورتها ، اعرض نظرية الهومومورفيزم للزمر .

<u>الحل</u>: سنتحقق أولاً من أن هذه المجموعة من الرواسم G تكون زمرة. ليكن لدينا الرواسم.

$\alpha_{a,b}$ ، $\alpha_{c,d}$ ، $\alpha_{e,f}$ لجميع $a,b,c,d,e,f \in \mathbb{R}$ ، $a \neq 0$ ، $c \neq 0$ ، $e \neq 0$

$$\alpha_{c,d} o \alpha_{a,b} : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto c(ax+b)+d = acx+bc+d \qquad (1)$$

وبالتالى فإن :
$$\alpha_{e,f} o (\alpha_{c,d} o \alpha_{a,b}) : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto eacx+ebc+ed+f$$

من (1) ينتج أن

$$\alpha_{cd} o \alpha_{a,b} = \alpha_{ac,bc+d} \qquad (2)$$

أى أن

$$\alpha_{e,f} o \alpha_{c,d} = \alpha_{ce,de+f}$$

وبالتالى فإن :

$$(\alpha_{e,f} o \alpha_{c,d}) o \alpha_{a,b}) : \mathbb{R} \to \mathbb{R}$$

$$x \mapsto ax + b \mapsto acex + bce + de + f$$

أى أن

$$\alpha_{e,f} o (\alpha_{c,d} o \alpha_{a,b}) = (\alpha_{ef} o \alpha_{c,d}) o \alpha_{a,b}$$

العنصر المحايد فى G هو

$$\alpha_{1,0} : \mathbb{R} \to \mathbb{R}$$

$$x \mapsto x$$

لأنه من (2) :

$$\forall \alpha_{a,b} \in G : \alpha_{1,0} o \alpha_{a,b} = \alpha_{1.a,1.b+0} = \alpha_{a,b}$$

معكوس $\alpha_{a,b}$ هو $\alpha_{\frac{1}{a},\frac{-b}{a}}$ لأن :

$$\forall \alpha_{a,b} \in G, a \neq 0 : \alpha_{\frac{1}{a},\frac{-b}{a}} o \alpha_{a,b} = \alpha_{\frac{1}{a}.a,\frac{b}{a}-\frac{b}{a}} = \alpha_{1,0}$$

أى أن G بالفعل زمرة .

سنثبت الآن أن θ هومومورفيزم

$$\forall a,c \in \mathbb{R} \setminus \{0\} \;\; \forall b,d \in \mathbb{R} : \theta(\alpha_{a,b} o \alpha_{c,d}) = \theta(\alpha_{ac,ad+b})$$

$$= \alpha_{ac,0} = \alpha_{a,0} o \alpha_{c,0} = \theta(\alpha_{a,b}) o \theta(\alpha_{c,d})$$

ونوجد نواة (θ) :

$$Ker(\theta) = \{\alpha_{a,b} \mid \alpha_{a,b} \in G, \theta(\alpha_{a,b}) = \alpha_{1,0}\}$$

$$= \{\alpha_{a,b} \mid \alpha_{a,b} \in G, \alpha_{a,0} = \alpha_{1,0}\}$$

$$= \{\alpha_{1,b} \mid b \in \mathbb{R}\}$$

ونوجد صورة (θ) :

$$\mathrm{Im}(\theta) = \{\alpha_{a,0} \mid a \in \mathbb{R}\}$$

وتنص نظرية الهوموмورفيزم هنا على أن :

$$\theta(G) \cong G / \{\alpha_{1,b} \mid b \in \mathbb{R}\}$$

$$\alpha_{a,0} \leftrightarrow \alpha_{a,c}\{\alpha_{1,b} \mid b \in \mathbb{R}\}, a \neq 0$$

أى أن

$$\alpha_{a,0} \leftrightarrow \{\alpha_{a,ab+c} \mid a,b,c \in \mathbb{R}, a \neq 0\}$$

أى أن

$$\alpha_{a,0} \leftrightarrow \{\alpha_{a,r} \mid a,r \in \mathbb{R}, a \neq 0\}$$

مثال ١٤: برهن على أن $\theta : (\mathbb{R}^*_+, .) \to (\mathbb{R}, +)$ (حيث $\mathbb{R}^*_+$ مجموعة الأعداد الحقيقية الموجبة (أكبر من الصفر) المعرف بـ $\theta(x) = \log_{10} x$ هومومورفيزم .
اوجد نواته ، صورته ، استخدم نظرية الهومومورفيزم لإثبات أن : $(\mathbb{R}^*_+, .) \cong (\mathbb{R}, +)$.

الحل:

$$\forall x, y \in \mathbb{R}^*_+ : \theta(x.y) = \log_{10} xy = \log_{10} x + \log_{10} y = \theta(x) + \theta(y)$$

أى أن θ هومومورفيزم .

$$Ker(\theta) = \{x \in \mathbb{R}^*_+ : \theta(x) = 0\}$$
$$= \{x \in \mathbb{R}^*_+ : \log_{10} x = 0\} = \{1\}$$

نبرهن الآن على أن $\theta(\mathbb{R}^*_+) = \mathbb{R}$ كالآتى :

$$\forall y \in \mathbb{R} \; \exists \; 10^y \in \mathbb{R}^*_+ : \log_{10} 10^y = y$$

أى أن $\theta(10^y) = y$

نطبق الآن نظرية الهومومورفيزم .

$$(\mathbb{R}^*_+, .) / \{1\} = (\mathbb{R}^*_+, .) / Ker(\theta) \cong \theta(\mathbb{R}^*_+, .) = (\mathbb{R}, +) \qquad (1)$$

والآن $\psi : (\mathbb{R}^*_+, .) \to (\mathbb{R}^*_+, .) / \{1\}$ أيزومورفيزم لأن : ψ راسم شامل (غامر) : واضح .

$$x \mapsto x\{1\} = \{x\}$$

ψ راسم واحد لواحد لأن :

$$\psi(x) = \psi(y) \Rightarrow \{x\} = \{y\}$$
$$\Rightarrow x = y \qquad \forall x, y \in \mathbb{R}^*_+$$

ψ هومومورفيزم لأن :

$$\psi(x.y)=\{x.y\}=\{x\}.\{y\}=\psi(x).\psi(y)$$

وبالتعويض فى (1) ينتج أن :

$$(\mathbb{R}_{+}^{*},.)\cong(\mathbb{R},+)$$

(انظر مثال ٢ فى بند (١-٣-٨))

مثال ١٥ : إذا كان $\varphi:G\to K$ هومومورفيزم زمر ، $|G|<\infty$ أى أن G منتهية فبرهن على أن $|\varphi(G)|$ (أى عدد عناصر $\varphi(G)$) يقسم $|G|$.

البرهان : من نظرية الهومومورفيزم : $G/Ker(\varphi)\cong\varphi(G)$ وبالتالى فإن :

(1) $\quad |G/Ker(\varphi)|=|\varphi(G)|$. ومن نظرية لاجرانج

$$|G|=|Ker(\varphi)|.[G:Ker(\varphi)]$$
$$=|Ker(\varphi)|\ \ |G/Ker(\varphi)| \qquad (2)$$

من (1) ، (2) ينتج المطلوب مباشرة .

مثال ١٦ : برهن على أن $\mathbb{Q}\not\cong\mathbb{Q}/\mathbb{Z}$ أى أن $\mathbb{Q}/\mathbb{Z}$ ، $\mathbb{Q}$ غير متشاكلتين .

البرهان : واضح أن العمليتين هما الجمع . لاحظ كذلك أن $\mathbb{Z}$ زمرة جزئية طبيعية فى $\mathbb{Q}$ لأنه لأى $q\in\mathbb{Q}$ ، ولأى $z\in\mathbb{Z}$:

$$-q+z+q=z\in\mathbb{Z}$$

لاحظ كذلك أن أى عنصر فى $\mathbb{Q}/\mathbb{Z}$ له رتبة منتهية لأن لكل $x\in\mathbb{Q}$:

$$x+\mathbb{Z}\in\mathbb{Q}/\mathbb{Z}\Rightarrow\exists p,q\in\mathbb{Z},q\neq0,(p,q)=1$$ (أى ليس لهما قواسم مشتركة سوى ±1)

بحيث إن : $\quad x+\mathbb{Z}=\frac{p}{q}+\mathbb{Z}$

والآن رتبة $x+\mathbb{Z}$ هى q لأن :

$$\underbrace{(\frac{p}{q}+\mathbb{Z})+\ldots+(\frac{p}{q}+\mathbb{Z})}_{q\ \text{من المرات}}=p+\mathbb{Z}=\mathbb{Z})$$ (العنصر المحايد فى $\mathbb{Q}/\mathbb{Z}$)

بينما لايوجد أى عنصر فى $\mathbb{Q}$ له رتبة منتهية سوى الصفر .

طريقة اخرى : ليكن $r \in \mathbb{Q} \setminus \{0\}$ ، وليكن $\varphi : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}$ هو الأيزومورفيزم الموجود .

عندئذ فإنه يوجد $s + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ بحيث إن

$$\varphi(s + \mathbb{Z}) = r, \quad s \notin \mathbb{Z}$$

(لاحظ أنه إذا كان $s \in \mathbb{Z}$ فمعنى هذا أن $s + \mathbb{Z} = \mathbb{Z}$ وهو العنصر المحايد فى $\mathbb{Q}/\mathbb{Z}$

صورته هى $r \neq 0$ ، فلا يكون φ أيزومورفيزم)

$s \in \mathbb{Z}$ ، كما سبق له رتبة منتهية ولتكن $t > 0$ أى أن :

$$t(s + \mathbb{Z}) = \mathbb{Z}$$

والآن لأن φ أيزومورفيزم فإن : ($\mathbb{Z}$ هو العنصر المحايد فى $\mathbb{Q}/\mathbb{Z}$) $0 = \varphi(\mathbb{Z})$

$$= \varphi(t(s + \mathbb{Z})) \quad = \quad t\varphi(s + \mathbb{Z}) = tr \neq 0$$

φ هومومورفيزم

وهذا تناقض .

مثال ١٧ : لتكن $(G, +)$ زمرة . برهن على أن :

$$\forall a \in G \quad \forall n \in \mathbb{N} : \quad -(na) = n(-a)$$

البرهان : باستخدام الاستقراء الرياضى :

عند $n = 0$: $0 = 0$

عند $n = 1$:

الطرف الأيمن $(L.H.S.) = -a = (R.H.S.)$ الطرف الأيسر

نفترض صحة الادعاء لكل $n \leq m$ $(*)$

نبرهن الآن على صحة الادعاء عند $n = m + 1$:

$$L.H.S. = -[(m+1)a] = -[\underbrace{a + \ldots + a}_{m+1 \text{ من المرات}}] = -(a + ma)$$

(لم نضع أقواساً لأن G زمرة أى يتحقق لها قانون المشاركة (أو الدمج))

$$\stackrel{1}{=} -ma - a \underset{(*)}{=} m(-a) - a = (m+1)(-a)$$

يتبقى أن نثبت (!) : لدينا :

$$-(a+ma)+(a+ma)=0 \qquad (1)$$

أيضاً لدينا :

$$-ma-a+a+ma=-ma+0+ma=0 \qquad (2)$$

من (1) $-(a+ma)$ معكوس $a+ma$ ، ومن (2) $-ma-a$ معكوس $a+ma$ ، ولكن المعكوس وحيد ، فينتج المطلوب مباشرة .

ملحوظة : فى الواقع ليست هناك ضرورة لإثبات (!) لأن $a,ma\in G$ وفى أية زمرة $(G,.)$: $(ab)^{-1}=b^{-1}a^{-1}$.

مثال ١٨ : اضرب مثالاً لزمرة قسمة G/N بحيث يكون $aN=bN$ حيث $a,b\in G$ ولكن رتبة $(a)\neq$ رتبة (b) .

الحل : فى الزمرة $\mathbb{Q}/\mathbb{Z}$ لدينا : $1+\mathbb{Z}=\mathbb{Z}=0+\mathbb{Z}$ لكن رتبة (0) هى الواحد بينما رتبة (1) $=\infty$.

مثال ١٩ : لتكن $G:=\mathbb{Z}/18\mathbb{Z}$ ، ولتكن $H:=[\bar{6}]=\{\bar{0},\bar{6},\overline{12}\}$. اسرد عناصر G/H ، واوجد رتبة $(\bar{5}+[\bar{6}])$ فى $\dfrac{\mathbb{Z}/18\mathbb{Z}}{[\bar{6}]}$.

الحل : عناصر $\dfrac{\mathbb{Z}/18\mathbb{Z}}{[\bar{6}]}$ هى : $[\bar{6}],\bar{1}+[\bar{6}],\bar{2}+[\bar{6}],\bar{3}+[\bar{6}],\bar{4}+[\bar{6}],\bar{5}+[\bar{6}]$

$$\underbrace{(\bar{5}+[\bar{6}])+\ldots+(\bar{5}+[\bar{6}])}_{\text{6 مرات}}=\overline{30}+[\bar{6}]=[\bar{6}]$$ أى أن $Ord(\bar{5}+[\bar{6}])\leq 6$

لكن $$\underbrace{(\bar{5}+[\bar{6}])+\ldots+(\bar{5}+[\bar{6}])}_{x\ \text{مرات}}\neq[\bar{6}]$$ لأى $x<6$ وبالتالى فإن $Ord(\bar{5}+[\bar{6}])=6$

انظر مثال (١-٧-٤) .

مثال ٢٠: لتكن H زمرة جزئية من الزمرة G بحيث إنه توجد بالضبط مجموعتان مشاركتان يسرايان مختلفتان من G بالنسبة إلى H . برهن على أن H زمرة جزئية طبيعية فى G .

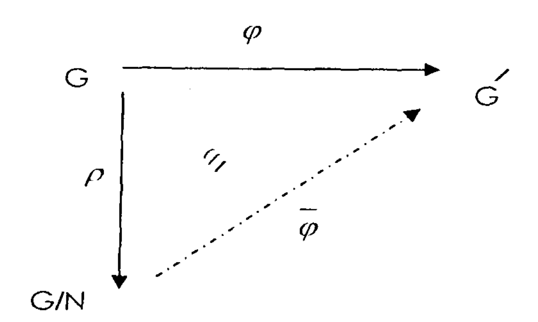
<u>البرهان</u> : لتكن $x \in G$. إذا كانت $x \in H$ فإن $xH = Hx$ (لأن كلتا المجموعتين المشاركتين $= H$) . إذا كانت $x \notin H$ فإن xH هى مجموعة جميع العناصر التى تقع فى G لكنها لاتقع فى H لأن :

$$z \in xH, x \notin H \Rightarrow z = xh, x \notin H, h \in H \Rightarrow x = zh^{-1}, h \in H$$

إذا كان $z \in H$ فإن $x \in H$ وهذا تناقض . إذن جميع عناصر xH لاتقع فى H .

ومن حيث إنه لاتوجد سوى مجموعتين مشاركتين يسرايين من G بالنسبة إلى H إحداهما H ومن حيث إن $xH \cap H$ هو المجموعة الخالية (نظرية المجموعات) ، فإن xH هى مجموعة **جميع** العناصر التى تنتمى إلى G ولا تنتمى إلى H . وبالمثل تكون Hx مجموعة **جميع** العناصر التى تقع فى G ولاتقع فى H وبالتالى يكون $xH = Hx$. إذن فى كلتا الحالتين $x \in H$ ، $x \notin H$ فإن $xH = Hx$ لجميع $x \in G$ وتكون H مجموعة جزئية طبيعية من G .

<u>مثال ٢١</u>: لتكن $\varphi : G \to G'$ هومومورفيزم زمر . N زمرة جزئية طبيعية من G ، $\rho : G \to G/N$ الإبيمورفيزم الطبيعى. اوجد الشرط الضرورى حتى يوجد هومومورفيزم زمر $\bar{\varphi} : G/N \to G'$ بحيث يكون الشكل الآتى إبدالياً



أى حتى يكون $\varphi = \bar{\varphi} o \rho$.

<u>الحـل</u> : من $\varphi = \bar{\varphi} o \rho$ ينتج أن :

$$\forall n \in N : \varphi(n) = (\bar{\varphi} o \rho)(n) = \bar{\varphi}(\rho(n)) \underset{n \in N}{=} \bar{\varphi}(N) = e'$$ (العنصر المحايد فى G')

(لأن $\bar{\varphi}$ هومومورفيزم ، N هو العنصر المحايد فى G/N ، (١-٣-٢) (أ)) .

$$\Rightarrow \quad N \subset Ker(\varphi)$$

<u>مثال ٢٢</u> : ليكن $\varphi: G \to G'$ هومومورفيزم زمر . N زمرة جزئية طبيعية فى G، $N \subset Ker(\varphi)$ ، $\rho: G \to G/N$ الإبيمورفيزم الطبيعى . عندئذ فإنه يوجد بالضبط هومومورفيزم وحيد

$$\bar{\varphi}: G/N \to G' \ , \ \varphi = \bar{\varphi} \circ \rho$$

وإذا كان φ إبيمورفيزماً فإن $\bar{\varphi}$ إبيمورفيزم كذلك ، $Ker(\bar{\varphi}) = Ker(\varphi)/N$.

<u>ملحوظة</u> : هذا المثال يظهر أن الشرط الضرورى الذى حصلنا عليه فى المثال ٢١ هو شرط كاف كذلك.

<u>البرهان</u> : (١) يوجد على <u>**الأكثر**</u> هومومورفيزم واحد $\bar{\varphi}$ يحقق الشرط المعطى لأن :

$$\bar{\varphi} \circ \rho = \varphi \Rightarrow \forall a \in G : \bar{\varphi}(aN) = \bar{\varphi}(\rho(a)) = (\bar{\varphi} \circ \rho)(a) = \varphi(a)$$

(٢) نبرهن على أنه يوجد بالفعل مثل هذا الهومومورفيزم

$$\begin{aligned} \bar{\varphi}: G/N &\to G' \\ aN &\mapsto \varphi(a) \end{aligned} \qquad \forall a \in G$$

لأن :

$$\forall a,b \in G : aN = bN \Rightarrow b^{-1}a \in N \underset{N \subset Ker(\varphi)}{\Rightarrow} e' = \varphi(b^{-1}a) = \varphi(b^{-1})\varphi(a) = \varphi(b)^{-1}\varphi(a)$$

$\Rightarrow \varphi(a) = \varphi(b) \Rightarrow \bar{\varphi}(aN) = \bar{\varphi}(bN)$ (e' هو العنصر المحايد فى G')

أى أن الراسم $\bar{\varphi}$ معرف جيداً .

(٣) الراسم $\begin{aligned} \bar{\varphi}: G/N &\to G' \\ aN &\mapsto \varphi(a) \end{aligned}$ لجميع $a \in G$ هومومورفيزم لأن :

$$\forall a,b \in G : \bar{\varphi}((aN)(bN)) = \bar{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(aN)\bar{\varphi}(bN).$$

(٤) ليكن φ راسماً غامراً (شاملاً) . إذن لكل $a' \in G'$ يوجد $a \in G$ بحيث يكون $a' = \varphi(a) = \bar{\varphi}(\rho(a))$. إذن $\bar{\varphi}$ راسم شامل (غامر) .

(٥) $\forall a \in G : aN \in Ker(\bar{\varphi}) \Leftrightarrow \bar{\varphi}(aN) = e' = \varphi(a) \Leftrightarrow a \in Ker(\varphi)$

$$\underset{(*)}{\Leftrightarrow} aN \in Ker(\varphi)/N$$

أى أن $Ker(\bar{\varphi}) = Ker(\varphi)/N$

(توضيح (*) : $a \in Ker(\varphi) \Leftarrow aN \in Ker(\varphi)/N$: مباشر . والآن :

$$aN \in Ker(\varphi)/N \Rightarrow \exists b \in Ker(\varphi) : aN = bN \Rightarrow b^{-1}a \in N \subset Ker(\varphi)$$

$$\underset{b \in Ker(\varphi)}{\Rightarrow} a \in Ker(\varphi))$$

<u>مثال ٢٣</u> : بإستخدام مثال ٢٢ برهن على أنه إذا كان $\varphi: G \to G'$ هومومورفيزم زمر فإن

$$\bar{\varphi} : G/Ker(\varphi) \to G' \qquad \forall a \in G$$
$$aKer(\varphi) \mapsto \varphi(a)$$

مونومورفيزم . كذلك فإن $G/Ker(\varphi) \cong \varphi(G)$.

<u>البرهان</u> : بوضع $N = Ker(\varphi)$ فى مثال٢٢ ينتج أنه يوجد هومومورفيزم وحيد $\bar{\varphi}$ يحقق الخاصة المعطاة . كذلك من المثال ٢٢ ينتج أن :

$$Ker(\bar{\varphi}) = Ker(\varphi)/Ker(\varphi) = \{aKer(\varphi) \mid a \in Ker(\varphi)\} = \{Ker(\varphi)\}$$

أى أن $Ker(\bar{\varphi})$ يحتوى على عنصر واحد هو $Ker(\varphi)$ وهو العنصر المحايد فى الزمرة $G/Ker(\varphi)$ وبالتالى فإن $\bar{\varphi}$ يكون راسماً واحداً لواحد (١-٣-٥ (أ)). ومن ثم فهو مونومورفيزم . وبالتالى فإن $G/Ker(\varphi) \cong \varphi(G)$ وهذه هى نظرية الهومومورفيزم مرة أخرى .

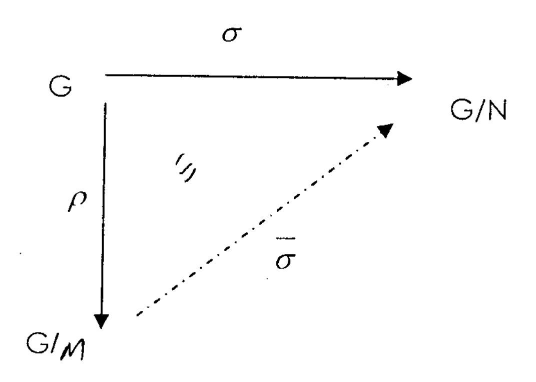
<u>مثال ٢٤</u> : استخدم مثال ٢٢ للبرهنة على أنه إذا كانت M، N زمرتين جزئيتين طبيعيتين من G، $M \subset N$ فإن :

(١) N/M زمرة جزئية طبيعية من G/M

(٢)
$$\varphi : (G/M)/(N/M) \to G/N \qquad \forall a \in G$$
$$(aM)(N/M) \mapsto aN$$

أيزومورفيزم .

<u>البرهان</u> : ليكن $\rho : G \to G/M$ ، $\sigma : G \to G/N$ الإبيمورفيزمين الطبيعيين .



لآن σ فوقى (شامل)، $M \subset N = Ker(\sigma)$ فمن مثال ٢٢ يوجد بالضبط إبيمورفيزم وحيد

١-٧-١

$\bar{\sigma} : G/M \to G/N$ بحيث إن الشكل (*) يكون إبدالياً . ولأن :

$$Ker(\bar{\sigma}) = Ker(\sigma)/M = N/M$$

ينتج أن N/M زمرة جزئية طبيعية من G/M .

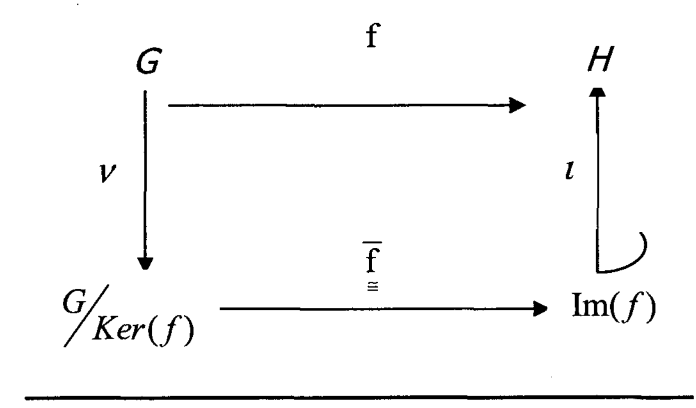
ومن نظرية الهومومورفيزم ينتج أن :

$$\frac{G/M}{N/M} = \frac{G/M}{Ker(\bar{\sigma})} \cong \bar{\sigma}(G/M) \quad = \quad G/N$$

$\bar{\sigma}$ شامل

$$(aM)/(N/M) \mapsto aN$$

<u>**مثال ٢٥**</u> : باستخدام النواة المشاركة المرتبية برهن على أنه إذا كان $f : G \to H$ هومومورفيزماً فإن التحليل الآتى يكون موجوداً



حيث $\nu(a) = aKer(f)$ لجميع $a \in G$ ، $\iota(x) = x$ لجميع $x \in \mathrm{Im}(f)$ ،

$$\overline{f}(aKer(f)) = f(a)$$

البرهان : سنكون الشكل الآتى :

$$Ker(f) \xrightarrow{\ \iota\ } G \xrightarrow{\ \nu\ } G/Ker(f) = Co\ker(\iota)$$

$$G \xrightarrow{\ f'\ } \mathrm{Im}(f), \qquad G/Ker(f) \xrightarrow{\ \exists_1 \overline{f}\ } \mathrm{Im}(f)$$

حيث $f'(a) = f(a) \quad \forall a \in G$

واضح أن f' راسم فوقى (شامل) (إبيمورفيزم) .

غامر (شامل) $\overline{f}(aKer(f)) = f'(a) = f(a) \Rightarrow \overline{f}$

$$\overline{f}(aKer(f)) = e \Leftrightarrow f'(a) = e \Leftrightarrow a \in Ker(f)$$

(e هو العنصر المحايد فى H)

$\Rightarrow \quad \overline{f}$ واحد لواحد ((١-٣-٥ (أ))

أى أن $\overline{f}$ تناظر أحادى ومن ثم $\overline{f}$ أيزومورفيزم

مثال ٢٦ : برهن على أن γ_7 لاتحتوى على زمرة جزئية رتبتها 11 .

<u>البرهان</u> : عددعناصر γ_n هو $n!$ وبالتالى فإن عدد عناصر γ_7 هو: 7.6.5.4.3.2.1 (انظر (١-٢-٥) مثال ٣) . ومن نظرية لاجرانج (١-١٠-٣) عدد عناصر (رتبة) أى زمرة جزئية من زمرة منتهية G يكون قاسماً لعدد عناصر (رتبة) G .

ولكن 11 لاتقسم !7 وإلا قسمت 1 أو ... أو 7 . وينتج المطلوب مباشرة .

<u>مثال ٢٧</u> : برهن على أنه إذا كانت G زمرة فإن الزمرة الجزئية من G المتولدة من مربعات عناصر G تكون زمرة جزئية طبيعية من G .

<u>البرهان</u> : لتكن S هى الزمرة الجزئية من G المتولدة من مربعات عناصر G .

ولتكن $x \in S$. عندئذ فإن : $x = s_1 s_2 \dots s_k$ حيث s_1 ، s_2 ، ... ، s_k مربعات عناصر أو معكوسات مربعات عناصر ، أى أن أياً منها له الشكل a^2 أو $(a^2)^{-1}$ (انظر (١-١١-٢)) . ولكن $(a^2)^{-1} = (a^{-1})^2$ وبالتالى فإنه يمكن القول بأنها جميعاً مربعات عناصر. والآن ليكن $g \in G$ ، عندئذ فإن :

$$g^{-1}xg = g^{-1}s_1 g g^{-1} s_2 g \dots g^{-1} s_k g = t_1 t_2 \dots t_k , t_i = g^{-1} s_i g.$$

ونثبت أنه لجميع $1 \le i \le k$ يكون t_i مربع عنصر من عناصر G كالآتى :

لأن $s_i = a_i^2$ حيث $a_i \in G$ فإن :

$$t_i = g^{-1}s_i g = g^{-1}a_i g g^{-1} a_i g = (g^{-1}a_i g)^2$$

أى أن t_i مربع عنصر من عناصر G وبالتالى فإن $g^{-1}xg \in S$ وتكون S زمرة جزئية طبيعية من G .

<u>مثال ٢٨</u> : يقال لزمرة جزئية H من زمرة جزئية G إنها <u>**مضبوطة**</u> (أو فعلية) (proper) إذا كانت $G \ne H \ne \{e\}$ حيث e هو عنصر G المحايد .

لتكن G زمرة رتبتها العدد الأولى p ، برهن على أن G لاتحتوى على زمر جزئية مضبوطة .

<u>البرهان</u> : من (١-١١-٧) (٢) G زمرة دائرية ومن (١-١١-١٢) فإنه لكل t قاسم لـــp توجد بالضبط زمرة جزئية واحدة من G لها الرتبة t . ولكن p له قاسمان فقط هما 1،p. وبالتالى فإن الزمرتين الوحيدتين الموجودتين فى G هما $\{ e \}$ ، G . أى أن G ليس لها زمر جزئية مضبوطة .

طريقة أخرى : انظر (١-١٠-٤)

مثال ٢٩ : لتكن G زمرة إبدالية . ليكن $x,y\in G$ بحيث إن $Ord(x)=r$ ، $Ord(y)=s$. برهن على أنه إذا كان s, r ليس لهما قواسم مشتركة (عدا ±1) فإن $Ord(xy)=rs$.

البرهان : لأن G إبدالية فإن :

$$(xy)^n=\underbrace{xy.xy\ldots xy}_{n \text{ من المرات}}=\underbrace{x.x\ldots x}_{n \text{ من المرات}}\;.\;\underbrace{y.y\ldots y}_{n \text{ من المرات}}=x^n y^n \quad \forall n\in\mathbb{N}$$

وبالتالى فإن :

$$(xy)^{rs}=x^{rs}.y^{rs}=(x^r)^s.(y^s)^r=e.e=e \quad (e \text{ العنصر المحايد فى } G)$$

وبالتالى فإن $Ord(xy)$ يقسم rs . (1)

والآن ليكن m هو رتبة xy وبالتالى فإن : $(xy)^m=e$ أى أن $x^m y^m=e$ (لأن G إبدالية) . ينتج أن : $x^m=y^{-m}$. ومن ثم فإن $e=(x^r)^m=y^{-mr}$ ومن ثم فإن s (= رتبة y) تقسم mr ، ولكن r, s ليس بينهما قواسم مشتركة أى أن s لاتقسم r ، إذن s تقسم m . وبالمثل يمكن إثبات أن r تقسم m . ومن حيث إن r, s ليس لهما قواسم مشتركة . إذن rs تقسم m (2) . من (1) ، (2) ينتج المطلوب مباشرة .

مثال ٣٠ : لتكن G الزمرة الدائرية ذات الرتبة ٤ المتولدة من المجموعة $\{a\}$. ولتكن $H=[a^2]$ (أى الزمرة الجزئية المتولدة من المجموعة $\{a^2\}$) ، (انظر ١-١١-٢) . اوجد جميع المجموعات المشاركة اليسرى من G بالنسبة إلى H . حقق أن أى مجموعتين مشاركتين يسرايين إما أن تنطبقا وإما لايكون بينهما عناصر مشتركة ، حقق كذلك أن اتحاد هذه المجموعات المشاركة هو G .

الحل : الزمرة G هى : $G=\{e,a,a^2,a^3\}$ (هى أيزومورفية مع الزمرة $\{1,i,i^2,i^3\}$ حيث $i=\sqrt{-1}$ وكذلك الزمرة $\mathbb{Z}/4\mathbb{Z}$) (e هو عنصر G المحايد) والزمرة الجزئية H هى : $H=\{a^2,e\}$.

المجموعات المشاركة اليسرى هى :

$$eH=e\{a^2,e\}=\{a^2,e\}=H,$$
$$aH=a\{a^2,e\}=\{a^3,a\},$$

$a^2H = a^2\{a^2,e\} = \{a^4,a^2\} = \{e,a^2\} = H,$
$a^3H = a^3\{a^2,e\} = \{a^5,a^3\} = \{a,a^3\} = aH$

أى أنه توجد فى الواقع مجموعتان مشاركتان يسرايان هما :

$$H = \{e,a^2\},$$
$$aH = \{a,a^3\}$$

واضح أن $H \cap aH = \phi$ ، $H \cup aH = G$.

مثال ٣١ : لتكن H هى الزمرة الجزئية التافهة من G، $H \neq G$. عين جميع المجموعات المشاركة اليمنى من G بالنسبة إلى H .

الحـــل : إذا كان $a \in G$ فإن : (e هو العنصر المحايد فى G)

$Ha = \{e\}a$
$= \{ea\} = \{a\}$

أى أن المجموعات المشاركة اليمنى تتكون كل منها من عنصر واحد من G .

مثال ٣٢: اوجد الزمرة الجزئية فى $(\mathbb{Q}\setminus\{0\},.)$ المتولدة من المجموعة {٢} .

الحـــل : معكوس 2 بالنسبة إلى العملية "." (عملية الضرب) هو 2^{-1} . وبالتالى فإن عناصر الزمرة الجزئية المتولدة من $\{2\}$ يكون لها أحد الشكلين 2^n أو 2^{-n} حيث $n \in \mathbb{N}$.

مثال ٣٣ : اوجد الزمرة الجزئية فى $(\mathbb{Q},+)$ المتولدة من $\{1\}$.

الحـــل : عناصر هذه الزمرة الجزئية تكون على الشكل $\underbrace{1+1+...+1}_{n \text{ من المرات}}$ أو $\underbrace{-1-1...-1}_{n \text{ من المرات}}$

حيث $n \in \mathbb{N}$ أى هى الزمرة $\mathbb{Z}$.

مثال ٣٤ : برهن على أنه يوجد عدد لانهائى من الزمر ، بحيث إنه لايوجد أيزومورفيزم (تشاكل) بين أى اثنتين منها .

الحـــل: زمر التبديلات γ_1 ، γ_2 ، γ_3 ، ... لايوجد أيزومورفيزم بين أى اثنتين منها. كذلك الزمر الدائرية $\mathbb{Z}$ ، $\mathbb{Z}/2\mathbb{Z}$ ، $\mathbb{Z}/3\mathbb{Z}$ ، ... .

مثال ٣٥ : إذا كان $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ عنصراً فى γ_4 ، فاوجد σ^3

الحـــل : لاحظ أن $\sigma = (1\ 2)(3\ 4)$ ومن ثم فإن

$\sigma^2 = (1\ 2)(3\ 4)(1\ 2)(3\ 4)$
$= (1\ 2)^2(3\ 4)^2 = ee = e$

حيث e هو العنصر المحايد فى $\gamma_4(=S_4)$.

ومن ثم فإن : $\sigma^3=\sigma\sigma^2=\sigma e=\sigma=(1\ 2)(3\ 4)$.

مثال ٣٦ : إذا كانت G زمرة دائرية ذات الرتبة n ، وكان p قاسماً لـــ n . فبرهن على أنه يوجد إبيمورفيزم من G على زمرة دائرية ذات الرتبة p . ما نواة هذا الإبيمورفيزم ؟

الحـل : نعلم من (١-١١-٨) أن أى زمرة دائرية من الرتبة n تكون أيزومورفيزمية مع الزمرة $\mathbb{Z}/n\mathbb{Z}$. ومن ثم فالمطلوب إثبات أنه يوجد إبيمورفيزم من $\mathbb{Z}/n\mathbb{Z}$ إلى $\mathbb{Z}/p\mathbb{Z}$.

والآن نعرف :

$$f:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$$
$$x+n\mathbb{Z}\mapsto x+p\mathbb{Z}$$

f معرف جيداً :

$$\forall x,y\in\mathbb{Z}:x+n\mathbb{Z}=y+n\mathbb{Z}$$
$$\Rightarrow x-y\in n\mathbb{Z}\Rightarrow\exists k\in\mathbb{Z}:x-y=nk$$
$$\underset{p|n}{\Rightarrow}x-y=plk,\ kl\in\mathbb{Z}$$

($p\,|\,n$ تعنى p تقسم n)

$$\Rightarrow x-y\in p\mathbb{Z}\Rightarrow x+p\mathbb{Z}=y+p\mathbb{Z}$$

أى أن $f(x+n\mathbb{Z})=f(y+n\mathbb{Z})$

f راسم فوقى (شامل ، غامر) : واضح

f هومومورفيزم

$$\forall x,y\in\mathbb{Z}:f(x+n\mathbb{Z}+y+n\mathbb{Z})$$
$$=f(x+y+n\mathbb{Z})=x+y+p\mathbb{Z}=x+p\mathbb{Z}+y+p\mathbb{Z}$$
$$=f(x+n\mathbb{Z})+f(y+n\mathbb{Z})$$

أى أن f إبيمورفيزم

مثال ٣٧ : برهن على أنه $(\mathbb{Q},+)\not\cong(\mathbb{R},+)$

البرهان : ليكن $\varphi:(\mathbb{Q},+)\to(\mathbb{R},+)$ أيزومورفيزم. وليكن $\varphi(1)=k$

والآن $k=\varphi(1)=\varphi(b\frac{1}{b})=\varphi(\underbrace{\frac{1}{b}+\ldots+\frac{1}{b}}_{b\ \text{من المرات}})=b\varphi(\frac{1}{b}),\quad b\neq 0$

$$\Rightarrow \varphi(\frac{1}{b}) = \frac{k}{b}$$

والآن :

$$\forall \frac{a}{b} \in \mathbb{Q}, b \neq 0 : \varphi(\frac{a}{b}) = \varphi(\underbrace{\frac{1}{b} + \ldots + \frac{1}{b}}) = a\varphi(\frac{1}{b}) = k\frac{a}{b}$$

a من المرات

إذا كان $k \in \mathbb{Q}$ فإن صورة (φ) $(\mathrm{Im}(\varphi))$ ستحتوى فقط على الأعداد الكسرية (النسبية). أما إن كانت $k \notin \mathbb{Q}$ فإن صورة φ ستحتوى فقط على الأعداد غير الكسرية (غير النسبية irrationals) بالإضافة إلى الصفر. فى الحالتين لايمكن أن تكون φ شاملة (غامرة) ، أى أنه لايوجد أيزومورفيزم .

مثال ٣٨ : برهن على أن $(\mathbb{R},+) \not\cong (\mathbb{R}\setminus\{0\},.)$

البرهان : ليكن $\varphi : (\mathbb{R},+) \to (\mathbb{R}\setminus\{0\},.)$ أيزومورفيزم. لأن φ راسم شامل (غامر) فإنه يوجد $y \in \mathbb{R}$ بحيث يكون $\varphi(y) = -1$.

والآن

$$-1 = \varphi(y) = \varphi(\frac{y}{2} + \frac{y}{2}) = [\varphi(\frac{y}{2})]^2$$

$$\Rightarrow \varphi(\frac{y}{2}) = \sqrt{-1} \notin \mathbb{R}$$

تناقض .

إذن لايوجد مثل هذا الأيزومورفيزم .

مثال ٣٩: لتكن G زمرة ، H زمرة جزئية من G دليلها فى $G = 2$. برهن على أن H زمرة جزئية طبيعية فى G .

البرهان : لكل $a \in G$ ، $a \notin H$: $aH \cup H = G$ ، $aH \cap H = \phi$ (لأن دليل H فى $G = 2$. ولأن $Ha \cap aH \ni a$ وكذلك فإن $Ha \neq H$) وهذا يقتضى أن $Ha = aH$. وبديهى أنه إذا كان $a \in H$ فإن $aH = Ha$. وبالتالى فإن H زمرة جزئية طبيعية فى G . (انظر مثال ٢٠ !).

مثال ٤٠ : لتكن M، N زمرتين جزئيتين طبيعيتين فى G بحيث إن $M\cap N=\{e\}$ حيث e هو العنصر المحايد فى G . برهن على أنه لكل $m\in M$ ولكل $n\in N$: $mn=nm$.

البرهان :

$$n^{-1}m^{-1}nm=n^{-1}(m^{-1}nm)\in N \quad \text{(لأن } N \text{ زمرة جزئية طبيعية فى } G)$$

$$=(n^{-1}m^{-1}n)m\in M \quad \text{(لأن } M \text{ زمرة جزئية طبيعية فى } G)$$

$$\underset{M\cap N=\{e\}}{\Rightarrow} n^{-1}m^{-1}nm=e\Rightarrow mn=nm$$

مثال ٤١ : برهن على أنه إذا كانت G زمرة دائرية لانهائية فإن لها فقط مولدين .

البرهان : من نظرية تفصيل الزمر الدائرية (١-١١-٨) أى زمرة دائرية لانهائية تكون متشاكلة (أيزومورفية) مع $\mathbb{Z}$، $\mathbb{Z}$ لها مولدان ± 1، ومن ثم فإن الزمرة G يكون لها مولدان

طريقة أخرى : ليكن a مولداً لــ G . ومن ثم فإن a يكون ذا رتبة لانهائية .

وتكون

$$G=\{\ldots,a^{-r},\ldots,a^{-1},e,a,\ldots,a^{r},\ldots\}$$

ليكن $a^{t}\in G$ مولداً آخر لــ G ، وعندئذ فإن

$$G=\{\ldots,a^{-2t},a^{-t},e,a^{t},a^{2t},\ldots\}$$

ولأن $a^{t+1}\in G$ فإن :

$$a^{t+1}=a^{rt},r\in\mathbb{Z}$$

$$\Rightarrow a^{t(1-r)+1}=e \quad (e \text{ عنصر } G \text{ المحايد})$$

ونظراً لأن a ليس ذا رتبة منتهية فإن :

$$t(1-r)+1=0\Rightarrow(r-1)t=1\Rightarrow t=\pm1$$

أى أنه إذا كان a مولداً فإنه يوجد مولد آخر وحيد هو a^{-1} .

مثال ٤٢ : برهن على أنه إذا كان N، M زمرتين جزئيتين طبيعيتين من G فإن NM زمرة جزئية طبيعية من G .

البرهان : تذكر أن $NM:=\{nm\mid n\in N,m\in M\}$

من (١-٦-١) NM زمرة جزئية طبيعية فى G إذا كان

$$\forall a\in G: aNMa^{-1}\subset NM$$

أى أن $\forall a\in G \quad \forall nm\in NM : anma^{-1}\in NM$

والآن :

$$a(nm)a^{-1}=(an)ma^{-1}=(ka)ma^{-1}, k\in N$$ (لأن N زمرة جزئية طبيعية فى G)

$$=k(am)a^{-1}=k(\ell a)a^{-1}, \ell\in M$$ (لأن M زمرة جزئية طبيعية فى G)

$$=(k\ell)aa^{-1}=k\ell e, k\ell\in NM$$ (e العنصر المحايد فى G)

$$=k\ell\in NM$$

<u>مثال ٤٣</u> : ينص قانون المشاركة (الدمج) العام على أنه إذا كانت $(G,.)$ زمرة ، وكانت a_1 ، ... ، a_n عناصر فى G فإن كل حواصل الضرب الممكنة لهذه العناصر مأخوذة بنفس الترتيب تكون متساوية. برهن على صحة القانون .

<u>البرهان</u> : سنعرف :

$$\prod_{i=1}^{1} a_i := a_1,$$

$$\prod_{i=1}^{r+1} a_i := (\prod_{i=1}^{r} a_i)a_{r+1}$$

سنقيم البرهان على صحة القانون بالاستقراء الرياضى .

سنبرهن اولاً على أن :

$$(\prod_{i=1}^{r} a_i)(\prod_{j=1}^{s} a_{r+j})=\prod_{k=1}^{r+s} a_k$$

هذا صحيح من التعريف عند $s=1$.

نفترض الآن أن هذا صحيح عند $s=m$ ، أى أن :

$$(\prod_{i=1}^{r} a_i)(\prod_{j=1}^{m} a_{r+j})=\prod_{k=1}^{r+m} a_k$$

عندئذ فإن :

$$(\prod_{i=1}^{r} a_i)(\prod_{j=1}^{m+1} a_{r+j}) = (\prod_{i=1}^{r} a_i)[(\prod_{j=1}^{m} a_{r+j})a_{r+m+1}]$$

التعريف

$$= [(\prod_{i=1}^{r} a_i)(\prod_{j=1}^{m} a_{r+j})]a_{r+m+1}$$

قانون المشاركة (الدمج)

$$= (\prod_{k=1}^{r+m} a_k)a_{r+m+1} = \prod_{k=1}^{r+m+1} a_k$$

فرض الاستقراء   التعريف

والآن نعتبر حاصل الضرب بأى طريقة وضع للأقواس لـ a_1 ، a_2 ، ... ، a_n .
سيكون هذا على الشكل bc حيث b، c حاصلاً ضرب بأى طريقة لوضع الأقواس
لـ a_1 ، a_2 ، ... ، a_t ؛ a_{t+1} ، a_{t+2} ، ... ، a_n على الترتيب .
ونفترض مرة أخرى أن قانون المشاركة (الدمج ، التجميع) العام صحيح لأى عدد أصغر من n .

وهكذا فإن :

$$b=\prod_{i=1}^{t} a_t , c=\prod_{j=t+1}^{n} a_j$$

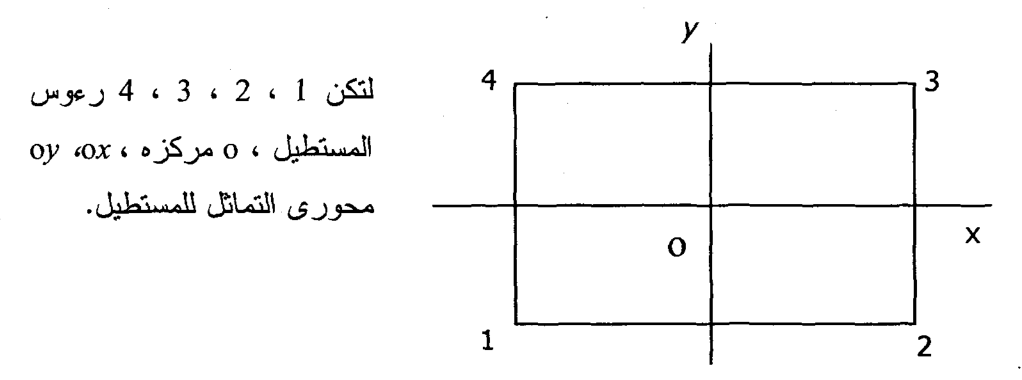
$$\Rightarrow bc=(\prod_{i=1}^{t} a_t)(\prod_{j=t+1}^{n} a_j)=\prod_{k=1}^{n} a_k$$

وتكون كل حواصل الضرب للعناصر a_1 ، a_2 ، ... ، a_n مأخوذة بنفس الترتيب متساوية وهى تساوى

$$\prod_{i=1}^{n} a_i$$

<u>مثال ٤٤</u> : زمرة كلاين الرباعية (انظر (١-٤-٤) مثال ٢) . تمثل هذه الزمرة هندسياً تماثلات المستطيل

لتكن 1 ، 2 ، 3 ، 4 رءوس المستطيل ، o مركزه ، ox، oy محورى التماثل للمستطيل.



هناك اربع تماثلات مختلفة ، هى :

(أ) الدوران حول النقطة o فى المستوى (مستوى المستطيل) بزاوية قدرها 0.

(ب) الدوران حول النقطة o فى المستوى بزاوية قدرها π

(جـ) الانعكاس حول ox

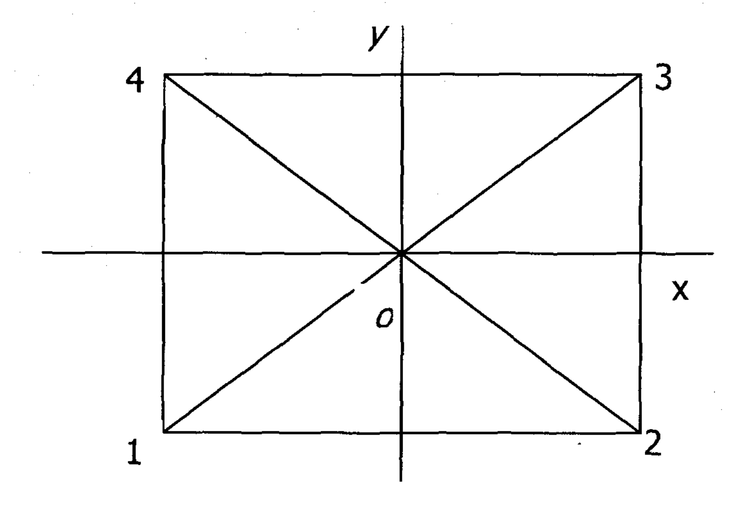
(د) الانعكاس حول oy

وهذه تناظر التبديلات الآتية على الترتيب :

(أ) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ (ب) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

(جـ) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ (د) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

<u>مثال ٤٥</u> : <u>الزمرة الثمانية</u> <u>Octic group</u>



تتكون هذه الزمرة من التماثلات بالنسبة للمربع . هناك أربعة دورنات حول o فى مستوى المربع بزاويا 0، $\frac{\pi}{2}$ ، π ، $\frac{3\pi}{2}$ التى تناظر على الترتيب :

$$e=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} ، \alpha=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} ، \alpha^2 ، \alpha^3$$

هناك أيضا أربعة انعكاسات حول أربعة خطوط تماثل ox، oy، 13، 24 التى تناظر على الترتيب :

$$\beta_1=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} ، \beta_2=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} ، \beta_3=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} ، \beta_4=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

تحقق من أن هذه العناصر الثمانية تكون زمرة . بوضع $\beta_1 = \beta$ يمكن التحقق من أن

$$\beta^2 = e = \alpha^4 ، \beta\alpha = \alpha^{-1}\beta ، \beta_2 = \alpha^2\beta ، \beta_3 = \alpha\beta ، \beta_4 = \alpha^3\beta$$

وتكون الزمرة هى :

$$\{e,\alpha,\alpha^2,\alpha^3,\beta,\alpha^2\beta,\alpha\beta,\alpha^3\beta\}$$

مثال ٤٦ : إذا كانت G زمرة بحيث إن $(ab)^n=a^nb^n$ لثلاثة أعداد صحيحة متتالية n، $n+1$، $n+2$ ولكل $a,b\in G$. فبرهن على أن G إبدالية .

البرهان : لدينا :

$$(ab)^n=a^nb^n \quad (1)\ ,\quad (ab)^{n+1}=a^{n+1}b^{n+1} \quad (2)\ ,\quad (ab)^{n+2}=a^{n+2}b^{n+2} \quad (3)$$

من (1) ، (2) ينتج أن :

$$a^{n+1}b^{n+1}=(ab)^{n+1}=(ab)^n(ab)=a^nb^nab$$

$\Rightarrow\ ab^n=b^na \quad (4)$ (بالضرب من اليسار واليمين للطرفين فى a^{-n} ، b^{-1})

ومن (1) ، (3) ينتج أن :

$$a^{n+2}b^{n+2}=(ab)^{n+2}=(ab)^n(ab)^2=a^nb^nabab$$

$\Rightarrow\ a^2b^{n+1}=b^naba \quad (5)$ (بالضرب من اليسار واليمين للطرفين فى a^{-n} ، b^{-1})

والآن من (4) ، (5) ينتج أن :

$$a^2b^{n+1}=b^naba=ab^nba=ab^{n+1}a$$

وبضرب الطرفين من اليسار فى a^{-1} نحصل على $\quad ab^{n+1}=b^{n+1}a \quad (6)$

ومن (4) ، (6) نحصل على :

$$ab^{n+1}=b^{n+1}a=bb^na=bab^n$$

وبضرب الطرفين من اليمين فى b^{-n} نحصل على : $\quad ab=ba$

أى أن G إبدالية .

مثال ٤٧ : لتكن G زمرة يتحقق لها $(ab)^2=(ba)^2$ لكل $a,b\in G$ ، ولكل $a\in G$: $[a^2=e\Rightarrow a=e]$. برهن على أن G إبدالية . (e عنصر G المحايد) .

البرهان : ليكن $a,b\in G$ لدينا :

$$a^2=((ab^{-1})b)^2=(b(ab^{-1}))^2=ba^2b^{-1}\Rightarrow a^2b=ba^2$$

وهذا معناه أيضاً أن : $\quad (a^{-1})^2b^{-1}=b^{-1}(a^{-1})^2 \qquad (*)$

كذلك فإن :

$$a^{-1}b^{-1}a=(a(a^{-1})^2)b^{-1}a=a((a^{-1})^2b^{-1})a$$
$$\underset{(*)}{=}a(b^{-1}(a^{-1})^2)a=ab^{-1}a^{-1} \qquad (**)$$

وبالمثل فإن : $\qquad b^{-1}a^{-1}b = ba^{-1}b^{-1} \qquad (***)$

ضع $c := aba^{-1}b^{-1}$ تحصل على :

$$c^2 = ab(a^{-1}b^{-1}a)ba^{-1}b^{-1} \underset{(**)}{=} ab(ab^{-1}a^{-1})ba^{-1}b^{-1} = aba(b^{-1}a^{-1}b)a^{-1}b^{-1}$$

$$\underset{(***)}{=} aba(ba^{-1}b^{-1})a^{-1}b^{-1} = (ab)^2(a^{-1}b^{-1})^2 = (ba)^2(a^{-1}b^{-1})^2$$

$$= (ba)^2(ba)^{-2} = e$$

ومن الفرض ينتج أن

$$aba^{-1}b^{-1} = c = e$$

وبالتالى فإن :

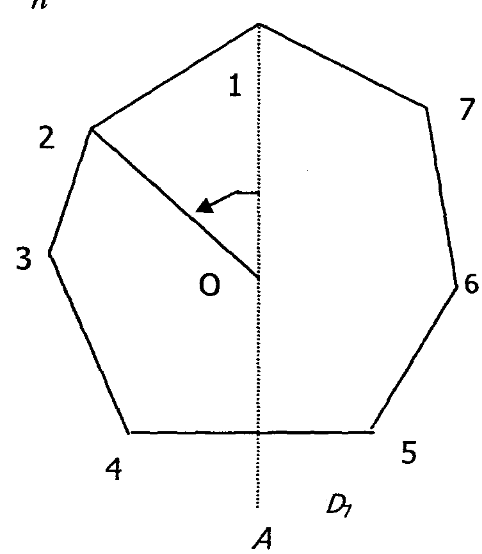
$$ab = ba$$

أى أن G إبدالية

مثال ٤٨ : الزمر الزوجية (الثنائية) Dihedral groups

الزمر الزوجية D_n هى زمرة التماثلات لمضلع منتظم له n من الأوجه . $D_n \subset \gamma_n (= S_n)$ ، تتولد من التبديلتين α ، β حيث $\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & \dots & 1 \end{pmatrix}$ ، $\beta = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & n & n\text{-}1 & \dots & 2 \end{pmatrix}$

وحيث تمثل α دورانا حول مركز المضلع ، بزاوية قدرها $\dfrac{2\pi}{n}$.



وتمثل β انعكاساً حول محور التماثل $AO1$. لاحظ أن D_2 هى زمرة كلاين الرباعية ((١-٤-٤) مثال٢) . واضح أن $\alpha^n = e = \beta^2$ حيث e عنصر الزمرة المحايد ، كذلك واضح أن $\alpha\beta = \beta\alpha^{-1}$. نبرهن الآن على أن D_n تتولد من $\{\alpha,\beta\}$:

إذا كانت x تنتمى إلى الزمرة الجزئية المتولدة من $\{\alpha,\beta\}$ فإن :

$$x = \alpha^{i_1}\beta^{j_1}\alpha^{i_2}\beta^{j_2}\ldots \qquad \text{(حاصل ضرب منته)},\ i_1,i_2,\ldots,j_1,j_2,\ldots\in\mathbb{Z}$$

لكن العلاقة $\beta\alpha = \alpha^{-1}\beta$ تختصر حاصل الضرب السابق إلى : $\alpha^{\lambda}\beta^{\mu},\ \lambda,\mu\in\mathbb{Z}$ الذى يمكن اختصاره كذلك إلى $\alpha^s\beta^t$ حيث $0\le s\le n-1$ ، $t = 0, 1$ ، وذلك باستخدام العلاقة $\alpha^n = e = \beta^2$. أى أننا انتهينا إلى أن أى عنصر x فى الزمرة المتولدة من المجموعة $\{\alpha,\beta\}$ يمكن التعبير عنه كالآتى :

$$x = \alpha^s\beta^t, 0\le s\le n-1, t=0 \quad \text{(or) أو} \quad t=1$$

ونبرهن الآن على أن هذه لـ $2n$ من العناصر كلها مختلفة ، لأن :

$$\alpha^{s_1}\beta^{t_1} = \alpha^{s_2}\beta^{t_2} \Rightarrow \alpha^{s_1-s_2} = \beta^{t_2-t_1} \Rightarrow \alpha^{s_1-s_2} = \begin{cases} e & ,t_2-t_1=0 \\ \beta & ,t_2-t_1=1 \end{cases}$$

إذا كان $\alpha^{s_1-s_2}=e$ فإن n يكون قاسماً لـ s_2-s_1 ولكن $|s_1-s_2|<n$ (لأن $0\le s\le n-1$) ومن ثم فإن $s_1-s_2=0$ وهذا يؤدى إلى $\beta^{t_1}=\beta^{t_2}$ أى أن $t_1=t_2$. أى أنه فى هذه الحالة يكون $s_1=s_2$ ، $t_1=t_2$. أما إذا كان $\alpha^{s_1-s_2}=\beta$ ، فإنه مع ملاحظة أن $\beta\alpha=\alpha^{-1}\beta$ يكون لدينا $\alpha^{s_1-s_2+1}=\alpha^{s_1-s_2-1}$ ، ومن ثم فإن $\alpha^2=e$ ، وهذا تناقض لأن $n>2$. أى أنه يكون لدينا فى النهاية

$\alpha^{s_1}\beta^{t_1}=\alpha^{s_2}\beta^{t_2}$ إذا كان وفقط إذا كان $s_1=s_2$ ، $t_1=t_2$ وهذا يبرهن على أن الـ $2n$ عنصراً ($2n$ هو عدد عناصر D_n)

$$\alpha^s\beta^t, 0\le s\le n-1, t=0 \quad \text{أو} \quad t=1$$

كلها مختلفة ، ومن ثم فإن الزمرة المتولدة من المجموعة $\{\alpha,\beta\}$ هى كل الزمرة الزوجية.

مثال٤٩: لتكن G زمرة. يعرف **مركز (G)** (centre of G) ويرمز له بالرمز $Z(G)$ بأنه:

$$Z(G) := \{a\in G: ax = xa \quad \forall a\in G\}$$

برهن على أن : (أ) $Z(G)$ زمرة جزئية طبيعية من G

(ب) زمرة الأوتومورفيزمات الداخلية (١-٣-٧) لــ G تكون متشاكلة (أيزومورفية) مع الزمرة $G/Z(G)$ (انظر مثال ٨ فى (١-٤-٤))

البرهان : (أ) الراسم

$$\varphi : G \to \gamma(G)$$
$$a \mapsto \varphi_a$$

هومومورفيزم زمر (١-٤-٤ مثال ١ (ب))

$$Ker(\varphi) = \{a \in G : \varphi_a = 1_G\}$$
$$= \{a \in G : \varphi_a(x) = 1_G(x) \quad \forall x \in G\}$$
$$= \{a \in G : axa^{-1} = x \quad \forall x \in G\}$$
$$= \{a \in G : ax = xa \quad \forall x \in G\} = Z(G)$$

(1_G هو راسم الوحدة من G إلى G أى أن : $\begin{matrix} 1_G : G \to G \\ a \mapsto a \end{matrix}$)

أى أن مركز G هو نواة هومومورفيزم ، ومن ثم فهو زمرة جزئية طبيعية من G .

(ب) لاحظ أن صورة (φ) ($\text{Im}(\varphi)$) هى زمرة كل الأوتومورفيزمات الداخلية لــ G .

ونطبق نظرية الهومومورفيزم (١-٨-١) فنحصل على :

$$\text{Im}(\varphi) \cong G/Ker(\varphi) = G/Z(G)$$

مثال ٥٠ : لتكن G زمرة . برهن على أن :

$$G/Z(G) \text{ دائرية } \Rightarrow G \text{ إبدالية}$$

البرهان : لاحظ أولاً أن $G/Z(G)$ زمرة لأن $Z(G)$ زمرة جزئية طبيعية فى G .

$G/Z(G)$ دائرية إذن لها مولد وليكن $xZ(G)$ حيث $x \in G$. هذا يقتضى أنه لكل $a,b \in G$:

يوجد $k, \ell \in \mathbb{Z}$ بحيث إن $aZ(G) = x^k Z(G)$ ، $bZ(G) = x^\ell Z(G)$. وهذا يقتضى أنه يوجد $z, y \in Z(G)$ بحيث إن : $a = x^k z$ ، $b = x^\ell y$. وبالتالى فإن :

$$ab = x^k z x^\ell y = x^{k+\ell} zy = x^\ell y x^k z = ba \quad \forall a,b \in G$$

أى أن G إبدالية .

مثال ٥١: لتكن G زمرة . لكل $a,b\in G$ يعرف **إبدالى a, b** (The commutator of a,b) ويرمز له بالرمز $[a, b]$ بأنه $[a,b]:=aba^{-1}b^{-1}$ ، وتعرف الزمرة الجزئية المتولدة من المجموعة $\{[a,b]:a,b\in G\}$ بأنها **زمرة إبداليات G** ويرمز لها بالرمز G' ويقال لها كذلك **الزمرة المشتقة** من G .

برهن على أن : (أ) $G'=\{e\} \Leftrightarrow$ إبدالية G .

(e كالمعتاد هو العنصر المحايد فى G)

(ب) $G'=\{[a_1,b_1]...[a_n,b_n]:n\in\mathbb{N}\setminus\{0\},a_1,...,a_n,b_1,...,b_n\in G\}$

البرهان : (أ) G إبدالية $\Leftrightarrow \forall a,b\in G: ab=ba$

$\Leftrightarrow \forall a,b\in G: aba^{-1}b^{-1}=e \Leftrightarrow G'=\{e\}$

(ب) لاحظ أن : $[a,b]^{-1}=bab^{-1}a^{-1}=[b,a]$

ومن (١-١١-٢) ينتج المطلوب مباشرة

مثال ٥٢ : برهن على أن G' زمرة إبداليات الزمرة G هى زمرة جزئية طبيعية من G .

البرهان : G' بالتعريف هى زمرة جزئية من G . يتبقى أن نثبت أنها "طبيعية" وذلك كالآتى :

$$\forall x\in G \quad \forall[a_1,b_1]...[a_n,b_n]\in G':$$

$$x[a_1,b_1]...[a_n,b_n]x^{-1}=$$

$$x[a_1,b_1]x^{-1}x[a_2,b_2]x^{-1}...x[a_n,b_n]x^{-1}$$

$$=xa_1b_1a_1^{-1}b_1^{-1}x^{-1}xa_2b_2a_2^{-1}b_2^{-1}x^{-1}...xa_nb_na_n^{-1}b_n^{-1}x^{-1}$$

$$=[xa_1x^{-1},xb_1x^{-1}][xa_2x^{-1},xb_2x^{-1}]...[xa_nx^{-1},xb_nx^{-1}]\in G'$$

مثال ٥٣ : لتكن N زمرة جزئية طبيعية من زمرة G . برهن على أن :

G/N إبدالية $\Leftrightarrow G'\subset N$

(وعلى وجه الخصوص : G/G' إبدالية).

البرهان : لتكن $G'\subset N$:

$$\forall a,b\in G: aN.bN = abN \underset{G'\subset N}{=} ab[b^{-1},a^{-1}]N = abb^{-1}a^{-1}baN$$

$$= baN = bN.aN \Rightarrow G/N$$ إبدالية

والآن لتكن G/N إبدالية . نعتبر الإبيمورفيزم الطبيعي

$$\rho: G\to G/N$$
$$a\mapsto aN$$

$$\forall a,b\in G: \rho([a,b]) = \rho(aba^{-1}b^{-1}) = \rho(a)\rho(b)\rho(a^{-1})\rho(b^{-1})$$

$$= \rho(a)\rho(b)\rho(a)^{-1}\rho(b)^{-1} \quad \underset{G/N \text{ إبدالية}}{=} \quad \rho(a)\rho(a)^{-1}\rho(b)\rho(b)^{-1}$$

$$= N \Rightarrow [a,b]\in Ker(\rho) = N$$
$$\Rightarrow \quad G'\subset N$$

(تذكر أن N عنصر G/N المحايد ، $Ker(\rho)=N$. انظر (١-٧-١))

<u>مثال ٥٤</u> : لتكن $A\subset G$ حيث G زمرة ، A مجموعة . **<u>يعرف ممركز A فى G</u>** : $C(A)$ (The centralizer) كالآتى :

$$C(A) := \{x : x\in G, \quad \forall a\in A: xa = ax\}$$

برهن على أن : (أ) $C(A)$ زمرة جزئية من G .

(ب) $A\subset G$ (زمرة جزئية إبدالية من G) $\Rightarrow A\lhd C(A)$

(زمرة جزئية طبيعية من $C(A)$)

<u>البرهان</u> : (أ) واضح أن عنصر G المحايد e ينتمى إلى $C(A)$ والآن :

$$x\in C(A)\Rightarrow \forall a\in A: xa = ax \Rightarrow \forall a\in A: ax^{-1} = x^{-1}a$$
$$\Rightarrow x^{-1}\in C(A)$$

كذلك فإن :

$$\forall x,y\in C(A): \forall a\in A: xa = ax, ya = ay$$
$$\Rightarrow xya \underset{y\in C(A)}{=} xay \underset{x\in C(A)}{=} axy \Rightarrow xy\in C(A)$$

أى أن $C(A)$ زمرة جزئية من G .

(ب) A زمرة جزئية إبدالية من $G \Leftarrow [a\in A\Rightarrow a\in C(A)]$

أى أن A زمرة جزئية من $C(A)$. يتبقى أن نثبت أن A "طبيعية" .

(من تعريف $C(A)$) $\forall x \in C(A) \quad \forall a \in A : xax^{-1} = axx^{-1} = a \in A$

زمرة جزئية طبيعية $\Rightarrow A \subset C(A)$.

مثال ٥٥ : لتكن G زمرة إبدالية . لتكن H مجموعة جزئية من G تتكون من عنصر G المحايد e ، كل عناصر G التى رتبتها = ٢ . برهن على أن H زمرة جزئية من G .

البرهان :

$$\forall a \in H : a^2 = e \Rightarrow \forall a \in H : a^{-1} = a \in H \qquad (1)$$

كذلك فإن :
$$\forall a,b \in H : ab = a^{-1}b^{-1} = (ba)^{-1} \underset{G \text{ إبدالية}}{=} (ab)^{-1}$$

$$\Rightarrow (ab)^2 = e \Rightarrow ab \in H \qquad (2)$$

من (1) ، (2) وكذلك $e \in H$ ينتج المطلوب مباشرة .

مثال ٥٦ : إذا اسقطنا كلمة "إبدالية" من مثال ٥٥ السابق مباشرة فهل تكون العبارة صائبة أيضاً ؟

الحل : العبارة فى هذه الحالة خاطئة . مثال مضاد : اعتبر $G = S_3 (= \gamma_3)$ ، $H = \{e, (12), (13), (23)\}$. H ليست زمرة جزئية فى G لأن : $(13)(12) = (123) \notin H$

تعرف $U(n)$ بأنها مجموعة كل الأعداد الصحيحة الموجبة (> 0) التى هى أصغر من n ، وليس بينها وبين n قواسم مشتركة سوى الواحد . عندئذ فإن $U(n)$ تكون زمرة مع عملية الضرب مقياس n.

مثال ٥٧ : برهن على أن $U(10) \not\cong U(12)$

البرهان :

$$U(12) = \{1,5,7,11\} \quad , \quad U(10) = \{1,3,7,9\}$$

$$1^2 \equiv 1(\text{mod}12), \quad 5^2 \equiv 1(\text{mod}12), \quad 7^2 \equiv 1(\text{mod}12), \quad 11^2 \equiv 1(\text{mod}12) \quad (*)$$

والآن ليكن $\varphi : U(10) \to U(12)$ تشاكلاً . ينتج أن :

$$\varphi(1) = \varphi(1.1) = \varphi(1).\varphi(1) = 1.1 = 1(\text{mod}12)$$

(من (*) جميع $x \in U(12)$ تحقق $x^2 \equiv 1\text{mod}(12)$) $\varphi(9) = \varphi(3.3) = \varphi(3)^2 \equiv 1(\text{mod}12)$

أى أن $\varphi(1) = \varphi(9)$ تناقض مع φ تشاكل

مثال ٥٨ : اختبر الراسم $\begin{aligned}\varphi:(\mathbb{R},+)&\to(\mathbb{R},+)\\ x&\mapsto x^5\end{aligned}$

هل φ تناظر أحادى ؟ هل φ أيزومورفيزم ؟

الحل :

$$\forall x,y\in\mathbb{R}:\quad \varphi(x)=\varphi(y)\Rightarrow x^5-y^5=0\Rightarrow x=y\in\mathbb{R}$$

أى أن φ واحد لواحد

$$\forall y\in\mathbb{R}\quad \exists\, y^{1/5}\in\mathbb{R}:\varphi(y^{1/5})=y$$

أى أن φ شامل (غامر)

لكن

$$\varphi(x+y)=(x+y)^5\neq x^5+y^5=\varphi(x)+\varphi(y)$$

(خذ مثلاً $x=1=y$)

أى أن φ ليس هومومورفيزم وبالتالى ليس تشاكلاً .

مثال ٥٩ : إذا كان $\varphi:G\to G'$ هومومورفيزماً فإنه لأى $a\in G$:

(رتبة $(\varphi(a))$ تقسم n) $\qquad Ord(a)=n\Rightarrow Ord(\varphi(a))\mid n$

البرهان : (العنصر المحايد فى G) $\qquad Ord(a)=n\Rightarrow a^n=e$

(e' العنصر المحايد فى G') $\qquad \Rightarrow\varphi(a)^n=\varphi(a^n)=e\Rightarrow Ord(\varphi(a))\mid n$

مثال ٦٠ : اختبر إذا ما كان $\begin{aligned}\varphi:\mathbb{Z}_{12}&\to\mathbb{Z}_{10}\\ \bar{x}&\mapsto\overline{3x}\end{aligned}$ هومومورفيزماً .

الحـــل :

$$\varphi(\bar{3})=\overline{3.3}=\bar{9}\Rightarrow\varphi(\bar{0})=\varphi(\overline{12})=\varphi(\bar{3}+\bar{3}+\bar{3}+\bar{3})$$
$$=\quad 4\varphi(\bar{3})=4(\bar{9})=\overline{36}=\bar{6}\neq\bar{0}$$

φ هومومورفيزم

تناقض مع (١-٣-٢ (أ)) . إذن φ ليس هومومورفيزماً .

مثال ٦١ : ليكن $\varphi:\mathbb{Z}_{30}\to\mathbb{Z}_{30}$ هومومورفيزماً ، وليكن $Ker(\varphi)=\{\bar{0},\overline{10},\overline{20}\}$.
إذا كان $\varphi(\overline{23})=\bar{6}$ فاوجد جميع العناصر التى صورتها $\bar{6}$.

الحـــل :

$$\bar{6}=\varphi(\overline{23})=\varphi(\bar{3}+\overline{20})=\varphi(\bar{3})+\varphi(\overline{20})=\varphi(\bar{3})+\bar{0}=\varphi(\bar{3})$$

وبالتالى فإن

$$\varphi(3)=\varphi(\overline{13})=\varphi(\overline{23})=\bar{6}$$

أى أن العناصر التى صورتها $\bar{6}$ هى : $\bar{3},\overline{13},\overline{23}$.

مثال ٦٢ : ليكن $\varphi:\mathbb{Z}/17\mathbb{Z}\to G$ هومومورفيزماً زمرياً لكنه غير واحد لواحد .

عين φ .

الحـــل : مادام φ ليس واحداً لواحد إذن نواة (φ) ليست هى مجموعة العنصر المحايد فى $\mathbb{Z}/17\mathbb{Z}$.

ولكن $Ker(\varphi)$ زمرة جزئية (طبيعية) من $\mathbb{Z}/17\mathbb{Z}$ وبالتالى فلها الشكل $m\mathbb{Z}/17\mathbb{Z}$ حيث m قاسم لـــ 17 . ومن حيث إن 17 عدد أولى ، نواة (φ) ليست هى مجموعة العنصر المحايد $0+17\mathbb{Z}$ فى $\mathbb{Z}/17\mathbb{Z}$ فتكون نواة (φ) هى $\mathbb{Z}/17\mathbb{Z}$ ويكون φ هو الراسم الصفرى.

مثال ٦٣ : عين جميع الهومومورفيزمات من $\mathbb{Z}_{20}$ إلى $\mathbb{Z}_{10}$. ماعدد الإبيمورفيزمات ؟.

الحـــل :الهومومورفيزم يتحدد تماماً إذا عرفنا صورة العنصر $\bar{1}\in\mathbb{Z}_{20}$ لأنه إذا كان $\varphi(\bar{1})=\bar{a}$ فإن الصور هى : $\varphi(\bar{x})=\overline{ax}$ $(\varphi(\bar{x})=\varphi\underbrace{(\bar{1}+\ldots+\bar{1})}_{x\text{ من المرات}}=\underbrace{\bar{a}+\ldots+\bar{a}}_{x\text{ من المرات}})$

والآن من نظرية لاجرانج (١-١٠-٣) يكون $Ord(\varphi(\bar{1}))$ قاسماً لـــ $10=Ord(\mathbb{Z}_{10})$.

كذلك من مثال ٥٩ السابق $Ord(\varphi(\bar{1}))$ يقسم $Ord(\bar{1})$ وهو 20 . إذن $Ord(\varphi(\bar{1}))$ يقسم كلاً من 10 ، 20 وبهذا يكون $Ord(\varphi(\bar{1}))=1,2,5\text{ or }10$

فى حالة $Ord(\varphi(\bar{1}))=1$ يكون $\varphi(\bar{1})=\bar{0}=\overline{10}$

فى حالة $Ord(\varphi(\bar{1}))=2$ يكون $\varphi(\bar{1})=\bar{5}$

فى حالة $Ord(\varphi(\bar{1}))=5$ يكون $\varphi(\bar{1})=\bar{2},\bar{4},\bar{6}\text{ or }\bar{8}$

فى حالة $Ord(\varphi(\bar{1}))=10$ يكون $\varphi(\bar{1})=\bar{1},\bar{3},\bar{7}\text{ or }\bar{9}$

أى أنه توجد 10 هومومورفيزمات

والآن $\bar{1}$ مولد للزمرة $\mathbb{Z}_{10}$ فمن الاستنتاج (١-١١-١١) يكون $\bar{3}$ ، $\bar{7}$ ، $\bar{9}$ كذلك مولدات لـــ $\mathbb{Z}_{10}$ ، وبهذا يكون عدد الإبيمورفيزمات المطلوبة هو 4 .

<u>مثال ٦٤</u> : لتكن $G:=\mathbb{Z}/[20]$ ، $H:=[4]/[20]$. اسرد عناصر H ، G/H

<u>الحل</u> :

$$H=\{0+[20],4+[20],8+[20],12+[20],16+[20]\}$$

$G/H=\dfrac{\mathbb{Z}/[20]}{[4]/[20]}$ وهذه تتشاكل مع $\mathbb{Z}/[4]=\mathbb{Z}/4\mathbb{Z}$ ، فنتوقع أن تكون G/H متكونة من أربعة عناصر وهى كالآتى :

$$G/H=\{0+[20]+H,1+[20]+H,2+[20]+H,3+[20]+H\}$$

ولاحظ أن :

$4+[20]+H=H \qquad$ (لأن $4+[20]\in H$)

$$5+[20]+H=1+[20]+H+4+[20]+H=1+[20]+H+H=1+[20]+H$$

$$6+[20]+H=2+[20]+H+4+[20]+H=2+[20]+H+H=2+[20]+H$$

$$7+[20]+H=3+[20]+H+4+[20]+H=3+[20]+H+H=3+[20]+H$$

$8+[20]+H=H \qquad$ (لأن $8+[20]\in H$)

وهكذا ...

<u>مثال ٦٥</u> : عين جميع الهومومورفيزمات من $\mathbb{Z}_n$ إلى $\mathbb{Z}_n$

<u>الحـــل</u> : لجميع $\bar{i}=\bar{1},\bar{2},...,\bar{n}$ الراسم $\begin{array}{c}\varphi:\mathbb{Z}_n\to\mathbb{Z}_n\\ \bar{1}\mapsto\bar{i}\end{array}$ هومومورفيزم !

<u>مثال ٦٦</u> : اعط مثالاً لبيان أنه فى زمرة القسمة G/H ، يمكن أن يحدث أن $aH=bH$ بينما رتبة $(a)\neq$ رتبة (b)

<u>الحـــل</u> : لنأخذ $G=H=S_3(=\gamma_3)$ ، $a=(12)$ ، $b=(123)$

$(12)S_3=S_3=(123)S_3$.
$Ord\,(12)=2$, $Ord\,(123)=3$

مثال ٦٧ : لتكن N زمرة جزئية طبيعية من زمرة G ، ولتكن H زمرة جزئية من G . بحيث إن N زمرة جزئية من H . برهن على أن H/N زمرة جزئية طبيعية من G/N إذا كانت وفقط إذا كانت H زمرة جزئية طبيعية من G .

البرهان : " $\Rightarrow$ " : فى برهان النظرية الثانية للأيزومورفيزم (١-٨-٣) .

" $\Leftarrow$ " : لتكن H/N زمرة جزئية طبيعية من G/N . عندئذ فإن :

$$(xN)^{-1}hNxN = x^{-1}NhNxN = x^{-1}NhxN$$

$$= x^{-1}hxN \in H/N, x \in G, h \in H$$

$$\Rightarrow \exists\, h' \in H, \exists\, n \in N : x^{-1}hx = h'n \in H \qquad (N \text{ زمرة جزئية من } H)$$

أى أن H زمرة جزئية طبيعية من G .

مثال ٦٨ : ليكن $\varphi : U(30) \to U(30)$ هومومورفيزماً ، $Ker(\varphi) = \{1,11\}$. إذا كان $\varphi(7) = 7$ فعين كل عناصر $U(30)$ التى صورها بـــ φ هى 7 .

الحـــل :

$$U(30) = \{1,7,11,13,17,19,23,29\}$$

$$\varphi(17) = \varphi(77) \qquad (\text{لأن } 77 \equiv 17 (\text{mod}\, 30))$$

$$= \varphi(11.7) = \varphi(11)\varphi(7) = 1.7 = 7$$

بالتجربة لاتوجد عناصر أخرى فى $U(30)$ تكون صورتها بـــ φ هى 7 باستثناء العنصر7، أى أن العناصر فى U(30) التى صورتها 7 هى 7، 17 فقط .

مثال ٦٩ : إذا كان $\varphi : U(40) \to U(40)$ هومومورفيزماً ، وكان $Ker(\varphi) = \{1,9,17,33\}$ ، وكان $\varphi(11) = 11$ ، فاوجد جميع عناصر $U(40)$ التى صورتها 11 .

الحـــل :

$$\varphi^{-1}(\{11\}) = 11\,Ker(\varphi) = 11\{1,9,17,33\} = \{3,11,19,27\}$$

(الحساب فى (mod 40))

(انظر كذلك مثال ٦٨ السابق مباشرة)

مثال ٧٠ :**تعريف**: نعرف دالة فاى لأويلر φ (Euler's phi function). لتكن $\phi(1)=1$ ، ولكل عدد صحيح $1<n$ لتكن $\phi(n)$ هى عدد الأعداد الصحيحة الموجبة التى أقل من (أصغر من) n وليس بينها وبين n قواسم مشتركة . لاحظ أن $Ord(U(n))=\phi(n)$.
برهن على أن عدد الهومومورفيزمات من $\mathbb{Z}_n$ إلى $\mathbb{Z}_k$ هو $\sum \phi(d)$ حيث يتم الجمع على جميع d القواسم المشتركة لـــ n، k .

البرهان : لكل d قاسم لـــ k توجد زمرة جزئية وحيدة فى $\mathbb{Z}_k$ لها الرتبة d وهذه الزمرة الجزئية تتولد من $\varphi(d)$ من العناصر . وأى هومومورفيزم من $\mathbb{Z}_n$ إلى زمرة جزئية فى $\mathbb{Z}_k$ يجب أن "يصور" 1 فى مولد لهذه الزمرة الجزئية . وعلاوة على هذا فإن رتبة صورة "1" يجب أن تقسم n ، (مثال ٥٩) ، ومن ثم البرهان .
طريقة أخرى ليست مختلفة تماماً عما سبق: من نظرية الأعداد الابتدائية Elementary Number Theory نعلم أن $\sum_{d|n,k} \phi(d)$ هو $gcd(n,k)$ القاسم المشترك الأعظم لـــ n، k .
ومن حيث إن $f(\bar{1})$ يحدد تماماً الراسم f من $\mathbb{Z}_n$ إلى $\mathbb{Z}_k$ ، $\bar{1}\in\mathbb{Z}_n$ ومن نظرية لاجرانج رتبة $(f(\bar{1}))$ قاسم لـــ k ، ومن مثال ٥٩ رتبة $(f(\bar{1}))$ قاسم لـــ n ينتج المطلوب مباشرة .

مثال ٧١: لتكن N زمرة جزئية طبيعية من زمرة G . استخدم الملحوظة (١-٦-٤(أ)) للبرهنة على أن كل زمرة جزئية من G/N سيكون لها الشكل K/N حيث K زمرة جزئية من G .

البرهان : ليكن $\varphi: G \to G/N$ ، $a \mapsto aN$ الإبيمورفيزم الطبيعى (انظر (١-٧-١) ، (١-٧-٢)).
لتكن $\overline{K}$ زمرة جزئية من G/N ، ولتكن K هى الصورة العكسية لـــ $\overline{K}$ بواسطة φ
أى أن $K := \varphi^{-1}(\overline{K})$. عندئذ فإن K ستكون زمرة جزئية من G (١-٤-٣) (ب)

$$K/N = \varphi(K) = \varphi(\varphi^{-1}(\overline{K}) = \overline{K}$$

φ شاملة

مثال ٧٢: لتكن $\mathbb{Z}[X]$ زمرة كثيرات الحدود فى X ذات المعاملات الصحيحة مع عملية الجمع . برهن على أن الراسم $\varphi:\mathbb{Z}[X]\to\mathbb{Z}$ ، $f\mapsto f(3)$ هومومورفيزم . صف هندسياً نواة (f) .

<u>الحـل</u> :

$$\forall f,g \in \mathbb{Z}[X] : \varphi(f+g) = (f+g)(3)$$

$$= f(3) + g(3) = \varphi(f) + \varphi(g) \Rightarrow \varphi$$ هومومورفيزم

$$Ker(\varphi) = \{f \in \mathbb{Z}[X] \mid \varphi(f) = f(3) = 0\}$$

$$= \{f \in \mathbb{Z}[X] \mid f = (X-3)g, \quad g \in \mathbb{Z}[X], \text{ degree } (g) = \text{degree } (f) - 1\}$$

تمثل هذه المجموعة هندسياً منحنيات فى المستوى تمر جميعها بالنقطة (3،0)

<u>مثال ٧٣</u> : لتكن G زمرة منتهية ولتكن $\mathbb{Z}_{10}$ صورة هومومورفيزمية لـــ G . بماذا يمكنك القول عن رتبة (G) ؟

<u>الحـل</u> : لدينا $\varphi . G \to \mathbb{Z}_{10}$ هومومورفيزم فوقى. ينتج من نظرية الهومومورفيزم (١-٨-١) أن $\mathbb{Z}_{10} = \varphi(G) \cong G/Ker(\varphi)$ ومن ثم فإنه ينتج من نظرية لاجرانج (١-١٠-٣) أن :

$$10 = Ord(\varphi(G)) = \frac{Ord(G)}{Ord(Ker(\varphi))} (= [G : Ker(\varphi)])$$

$$\Rightarrow Ord(G) = 10.Ord(Ker(\varphi))$$

<u>مثال ٧٤</u> : لتكن N زمرة جزئية طبيعية من زمرة G . برهن على أن رتبة العنصر gN فى G/N تقسم رتبة العنصر g فى G .

<u>البرهان</u> : $\varphi : G \to G/N$ هومومورفيزم
$g \mapsto gN$

من مثال ٥٩ رتبة $(\varphi(a))$ تقسم رتبة (a) حيث $\varphi : G \to G'$ هومومورفيزم وينتج المطلوب مباشرة.

<u>مثال ٧٥</u> : لتكن $\mathbb{Z}_{10}$ ، $\mathbb{Z}_{15}$ صورتين هومومورفيزميتين لزمرة منتهية G . بماذا يمكنك القول عن رتبة (G) ؟

<u>الحـل</u> :من مثال٧٣: رتبة (G) مضاعف لرتبة $\mathbb{Z}_{10}$ ، مضاعف لرتبة $\mathbb{Z}_{15}$ ، ومن ثم فإن رتبة (G) تكون مضاعفاً لـــ30 (حيث 30 هى المضاعف المشترك الأصغر لـــ10، 15).

مثال ٧٦ : لتكن N زمرة جزئية طبيعية من زمرة منتهية G . إذا كان G/N بها عنصر رتبته n فاثبت أن G بها عنصر رتبته n . اعط مثالاً لبيان أن افتراض أن G منتهية شرط ضرورى .

البرهان : ليكن $Ord(gN)=n\in\mathbb{N}$ حيث $g\in G$. ينتج من مثال ٧٤ أن $Ord(g)=mn$ ، حيث $m\in\mathbb{N}$. وبالتالى فإن $Ord(g^m)=n$. إذا كانت G غير منتهية خذ $G=\mathbb{Z}$ ، $N=2\mathbb{Z}$ ، $\bar{1}\in \mathbb{Z}/2\mathbb{Z}$ ، $Ord(\bar{1})=2$ بينما لايوجد أى عنصر فى $\mathbb{Z}$ رتبته 2 .

مثال ٧٧ : إذا كانت N زمرة جزئية طبيعية من G ، وكانت $Ord(G/N)=m$. فبرهن على أن $x^m\in N$ لجميع $x\in G$.

البرهان : من نظرية لاجرانج (أو من النتيجة (١-١١-٩)) :

$$Ord(G/N)=m \Rightarrow Ord(xN)\mid m \quad \forall x\in G$$

$$\Rightarrow (xN)^m=N \qquad \forall x\in G$$

أى أن $x^mN=N$ لجميع $x\in G$ وهذا يقتضى أن $x^m\in N$ لجميع $x\in G$ (انظر تمهيدية (١-٥-٢)) .

مثال ٧٨ : برهن على أنه إذا كانت G زمرة غير إبدالية فإن $Aut(G)$ تكون غير دائرية .

البرهان : من مثال ٥٠ : G غير إبدالية $\Leftarrow$ $G/Z(G)$ ليست دائرية . ومن مثال ٤٩ $Int(G)\cong G/Z(G)$ وبالتالى فإن $Int(G)$ (زمرة الأوتومورفيزمات الداخلية لــ G) ليست دائرية . ومن النظرية (١-١١-٧) حيث إن $Int(G)$ زمرة جزئية من $Aut(G)$ ينتج أن $Aut(G)$ غير دائرية .

مثال ٧٩ : لتكن N زمرة جزئية طبيعية من زمرة منتهية G . إذا كان $gcd(Ord(x),Ord(G/N))=1$ القاسم المشترك الأعظم ، فبرهن على أن $x\in N$.

البرهان : $gcd(Ord(x),Ord(G/N))=1 \Rightarrow gcd(Ord(xN),Ord(G/N))=1$

ولكن $Ord(xN)$ يقسم $Ord(G/N)$ وبالتالى فإن $Ord(xN)=1$ ، أى أن $xN=N$ ومن ثم فإن $x\in N$ (تمهيدية (١-٥-٢))

مثال ٨٠ : قرر إذا ما كانت الرواسم الآتية هومومورفيزمات. إذا كانت كذلك فاوجد النواة فى كل حالة :

(أ) $\varphi:\mathbb{Z}\to\mathbb{R},\quad \varphi(n)=n$

(ب) $\varphi:\mathbb{Z}_6\to\mathbb{Z}_2$

$x\mapsto\varphi(x)$ = الباقى من x عند القسمة على 2 بالمفهوم الشائع

(جـ) $\varphi:\mathbb{Z}_9\to\mathbb{Z}_2$

$x\mapsto\varphi(x)$ = الباقى من x عند القسمة على 2 بالمفهوم الشائع

الحل : (أ)

$$\forall\ m,n\in\mathbb{Z}:\quad \varphi(m+n)=m+n=\varphi(m)+\varphi(n)$$

$\Rightarrow$ φ هومومورفيزم

$$Ker(\varphi)=\{x\in\mathbb{Z}:\varphi(x)=x=0\}=\{0\}$$

(ب) اعتبر $X=\{\bar{0},\bar{2},\bar{4}\}$ ، $Y=\{\bar{1},\bar{3},\bar{5}\}$

$$\left.\begin{aligned}&\forall x,y\in X: \quad \varphi(x+y)=\bar{0}=\bar{0}+\bar{0}=\varphi(x)+\varphi(y)\\&\forall x,y\in Y: \quad \varphi(x+y)=\bar{0}=\bar{1}+\bar{1}=\varphi(x)+\varphi(y)\\&\forall x\in X\forall y\in Y:\varphi(x+y)=\bar{1}=\bar{0}+\bar{1}=\varphi(x)+\varphi(y)\end{aligned}\right\rangle \ \varphi \text{ هومومورفيزم}$$

$$Ker(\varphi)=\{\bar{0},\bar{2},\bar{4}\}$$

(جـ) تناقض $\bar{0}=\varphi(\overline{10})=\varphi(\bar{1})=\bar{1}$

إذن φ ليس هومومورفيزماً .

مثال ٨١: كم عدد الهومومورفيزمات :

(أ) من $\mathbb{Z}$ إلى $\mathbb{Z}$ وشامل (غامر – فوقى)

(ب) من $\mathbb{Z}$ إلى $\mathbb{Z}_2$

(جـ) من $\mathbb{Z}$ إلى $\mathbb{Z}_2$ وغامر

(د) من $\mathbb{Z}$ إلى $\mathbb{Z}_8$

(هـ) من $\mathbb{Z}$ إلى $\mathbb{Z}_8$ وغامر

(و) من $\mathbb{Z}_{12}$ إلى $\mathbb{Z}_5$ وغامر

(ز) من $\mathbb{Z}_{12}$ إلى $\mathbb{Z}_6$

(ح) من $\mathbb{Z}_{12}$ إلى $\mathbb{Z}_6$ وشامل

(ط) من $\mathbb{Z}_{12}$ إلى $\mathbb{Z}_{14}$

(ى) من $\mathbb{Z}_{12}$ إلى $\mathbb{Z}_{16}$

<u>الحل</u> : (أ) يتحدد الهومومورفيزم تماماً بصورة المولد 1 ، كما جاء فى مثال ٦٣. وحتى يكون الهومومورفيزم فوقياً أى غامراً أو شاملاً كل $\mathbb{Z}$ (النطاق المصاحب) فيجب أن يكون $\varphi(1)=1$ أو $\varphi(1)=-1$. أما فيما عدا ذلك فلن يكون الهومومورفيزم شاملاً . فإذا كان $\varphi(1)=n$ مثلاً فستكون صورة (φ) هى $\{mn \mid m\in\mathbb{Z}\}$ فإذا كانت $n\neq\pm1$ فلن تكون صورة φ هى $\mathbb{Z}$.

(ب) هومومورفيزمان يعرفان بـ $\varphi(1)=\bar{0}$ ، $\varphi(1)=\bar{1}$

(حـ) هومومورفيزم واحد يعرف بـ $\varphi(1)=\bar{1}$

(د) ثمانية هومومورفيزمات $\varphi(1)=\bar{i}, \bar{i}\in\{\bar{0},\bar{1},\dots,\bar{7}\}$

(هـ) الهومومورفيزمات أربعة تعطى بـ $\varphi(1)=\bar{1}, \varphi(1)=\bar{3}, \varphi(1)=\bar{5}, \varphi(1)=\bar{7}$

لاحظ أن $\mathbb{Z}_8$ دائرية ورتبتها 8 ، وانظر الاستنتاج (١-١١-١١)

(و) من نظرية الهومومورفيزم (١-٨-١) ينتج أن

$$\mathbb{Z}_5=\varphi(\mathbb{Z}_{12})\cong \mathbb{Z}_{12}/Ker(\varphi) \Rightarrow 12=Ord(\mathbb{Z}_{12})=Ord(\mathbb{Z}_5).Ord(Ker(\varphi))$$
$$=5.Ord(Ker(\varphi))$$

تناقض لأن 5 لايقسم 12 . إذن لايوجد هومومورفيزم غامر من $\mathbb{Z}_{12}$ إلى $\mathbb{Z}_5$.

(ز) ستة هومومورفيزمات $\varphi(\bar{1})=\bar{i}, \bar{i}\in\{\bar{0},\bar{1},\dots,\bar{5}\}$ (انظركذلك (ط) ، (ى))

(ح) مثل (هـ) هناك هومومورفيزمان فقط $\varphi(\bar{1})=\bar{5}$ ، $\varphi(\bar{1})=\bar{1}$

انظر الإستنتاج (١-١١-١١) . يجب أن تكون صورة $\bar{1}$ مولدة لـ $\mathbb{Z}_6$ التى رتبتها 6 .

(ط) إذا كان $\varphi(\bar{1}) = \bar{n}$ فإنه يجب أن يتحقق :

$$\varphi(\bar{0}) = \varphi(\overline{12}) = \overline{12}\varphi(\bar{1}) = \overline{12n} = \overline{14k} = \bar{0}, k \in \mathbb{Z}$$
$$\Rightarrow \bar{n} = \bar{0}, \bar{n} = \bar{7}$$

أى أنه يوجد هومومورفيزمان

(ى) مثل (ط) إذا كان $\varphi(\bar{1}) = \bar{n}$ فإنه يجب أن يتحقق :

$$\varphi(\bar{0}) = \varphi(\overline{12}) = \overline{12}\varphi(\bar{1}) = \overline{12n} = \overline{16k} = \bar{0}, k \in \mathbb{Z}$$

ويتضح أن $\bar{n} = \bar{0}, \bar{4}, \bar{8}, \overline{12}$

أى أنه يوجد أربعة هومومورفيزمات .

<u>مثال ٨٢</u> : لتكن G زمرة إبدالية عنصرها المحايد e ، n عدداً صحيحاً . برهن على أن المجموعة $H =: \{x \in G : x^n = e\}$ زمرة من G . واضرب مثالاً لزمرة G فيها مجموعة كل عناصر G التى تحقق $x^2 = e$ لاتكون زمرة جزئية من G .

<u>الحـل</u> : $e^n = e$ يقتضى أن $e \in H$ أى أن H مجموعة ليست خالية . والآن ليكن $x, y \in H$ هذا يقتضى أن $x^n = e = y^n$. والآن :

$$(xy^{-1})^n = \underbrace{xy^{-1} \ldots xy^{-1}}_{} \quad = \quad x^n (y^{-1})^n = x^n (y^n)^{-1} = ee^{-1} = e$$

G إبدالية n من المرات

وبالتالى فإن $xy^{-1} \in H$ وينتج من (١-٤-٢) أن H زمرة جزئية من G .

المثال : $H = \{e, (12), (13), (23)\} \subset S_3$

$(12)(13) = (132) \notin H$. إذن H ليست زمرة جزئية من S_3 . لاحظ أن S_3 ليست إبدالية .

<u>مثال ٨٣</u> : لتكن G زمرة تحتوى على زمرتين جزئيتين طبيعيتين M، N . و لتكن H زمرة جزئية من G . برهن على أن :

$$HM/M \cong HN/N$$

إذا كان $H \cap M = H \cap N$

البرهان : من النظرية الأولى للأيزومورفيزم

$$HM/M \cong H/H \cap M = H/H \cap N \cong HN/N$$

(لاحظ أنه من (١-٣-٢) تركيب هومومورفيزمين يكون كذلك هومومورفيزماً ، ومعلوم أن تركيب تناظرين أحاديين هو تناظر أحادى ــ وبالتالى فإن تركيب أيزومورفيزمين هو كذلك أيزومورفيزم وبالتالى فإن $HM/M \cong HN/N$) .

مثال ٨٤ : لتكن G زمرة ، $N \lhd G$ (زمرة جزئية طبيعية فى G) . لتكن N إبدالية ، G/N كذلك إبدالية ، H زمرة جزئية من G . برهن على أنه توجد زمرة جزئية H_1 من H بحيث إن $H_1 \lhd H$ ، H/H_1 ، H_1 إبداليتان .

البرهان : نعرف $H_1 := H \cap N$. عندئذ فمن نظرية الأيزومورفيزم الأولى :

$$H/H_1 = H/H \cap N \cong HN/N, H_1 = H \cap N \lhd H$$

لكن $HN/N \subset G/N$ ، G/N إبدالية فينتج أن HN/N إبدالية ، ومن ثم فإن H/H_1 إبدالية . ومن حيث إن N إبدالية ، $H_1 \subset N$ فينتج أن H_1 إبدالية .

تمارين عامة

(١) ليكن $f : G \to H$ هومومورفيزم زمر . برهن على أن :

(أ) f مونورمورفيزم $\Leftrightarrow$ [$\forall K$ زمرة $\forall g,h : K \to G$ هومومورفيزمين $fg = fh \Rightarrow g = h$]

(ب) f إبيمورفيزم $\Leftarrow$ [$\forall K$ زمرة $\forall g,h : H \to K$ هومومورفيزمين $gf = hf \Rightarrow g = h$]

(٢) لتكن G زمرة دائرية رتبتها n . اعتبر هومومورفيزم الزمر : $\hat{d} : G \to G$, $x \mapsto x^d, d \in \mathbb{N}$

لتكن $G^d := \mathrm{Im}(\hat{d}) \subset G$ (لا تخلط هذه مع حاصل الضرب الكارتيزى!). برهن على أن :

$$G/G^d \cong \gcd(n,d)\mathbb{Z}$$

(٣) يقال لزمرة G إنها **دائرية محلية** (local cyclic) إذا كانت كل زمرة جزئية منتهية التولد(finitely generated) (أى عدد مولداتها منته) من G تكون دائرية. برهن على أن:

(أ) كل زمرة دائرية محلية تكون إبدالية .

(ب) إذا كانت G دائرية محلية ، وكانت U زمرة جزئية من G فإن U، G/U تكونان دائريتين محليتين .

(جـ) كل زمرة دائرية تكون دائرية محلية .

(د) $\mathbb{Q}$ ، $\mathbb{Q}/\mathbb{Z}$ دائريتان محليتان (بالنسبة لعملية الجمع)

(٤) لتكن G دائرية محلية ، وليكن $f,g : G \to G$ هومومورفيزمى زمر .

برهن على أن : $fg = gf$.

(٥) ليكن $p > 2$ عدداً أولياً ، $n \geq 1$ عدداً طبيعياً ، ولتكن $G[p^n] := U(\mathbb{Z}/[p^n])$

(انظر مثال ٥٧ من أمثلة متنوعة). برهن على أن :

(أ) $k \geq 0$ $\Leftarrow$ $(1+p)^{p^k} \equiv 1 + p^{k+1} (\mathrm{mod}\, p^{k+2})$

(ب) رتبة $\overline{(1+p)}$ فى $G[p^n]$ هى p^{n-1}

(إرشاد : استخدم (أ))

(٦) برهن على أنه لايوجد تشاكل (أيزومورفيزم) بين $(\mathbb{Q},+)$ ، $(\mathbb{Q}_+^*,.)$ (زمرة كل الأعداد الكسرية (النسبية) التى أكبر من الصفر)

(٧) برهن على أن المجموعة xHx^{-1} زمرة جزئية من G لجميع $x \in G$ إذا كانت وفقط إذا كانت H زمرة جزئية من G .

(٨) برهن على أنه لأية زمرة جزئية معكوسات عناصر مجموعة مشاركة يسرى تكون مجموعة مشاركة يمنى .

(٩) إذا كانت H زمرة جزئية من زمرة G بحيث كان دليل H فى G هو 2 . فبرهن على أن كل مجموعة مشاركة يمنى (يسرى على الترتيب) تكون مجموعة مشاركة يسرى (يمنى على الترتيب)

(١٠) برهن على أن أية زمرة لايمكن كتابتها كاتحاد زمرتين جزئيتين فعليتين

(١١) برهن على التبديلات على {4، 3، 2، 1} التى تترك كثيرة الحدود $x_1x_2+x_3+x_4$ كما هى تكون زمرة جزئية من S_4 ، ورتبتها 4 .

(١٢) لتكن H زمرة جزئية من G ، وليكن $x,y \in G$. سنعرف العلاقة $x \sim y$ إذا كان $x^{-1}y \in H$. برهن على أن هذه العلاقة علاقة تكافؤ على G وكذلك صف كل فصل تكافؤ.

(١٣) لتكن $S := \mathbb{R} \setminus \{-1\}$. نعرف * على S كالآتى :

$$\forall a,b \in S : a*b := a+b+ab$$

أ) برهن على أن $(S,*)$ زمرة

ب) حل المعادلة $2*\ x*3=7$ فى S

(١٤) ليكن $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$. نعرف * على $\mathbb{R}^*$ كالآتى :

$$\forall a,b \in \mathbb{R}^* : a*b := |a|b$$

(أ) برهن على أن * هى عملية تشاركية (إدماجية ، جمعية) على $\mathbb{R}^*$

(ب) برهن على أنه يوجد عنصر محايد أيسر بالنسبة إلى * (أى أنه يوجد $x \in \mathbb{R}^*$ بحيث إن $\forall a \in \mathbb{R}^* : x*a=a$) ، كما أنه يوجد معكوس أيمن لكل عنصر فى $\mathbb{R}^*$ (أى أنه يوجد $b \in \mathbb{R}^*$ بحيث إن $a*b=x$)

(جـ) هل $(\mathbb{R}^*,*)$ زمرة ؟

(د) علام يدل هذا المثال ؟

(١٥) بواسطة ضرب مثال برهن على أنه يمكن أن يكون للمعادلة $x^2 = e$ أكثر من حلين فى زمرة G عنصرها المحايد e .

(١٦) أى هذه الرواسم يكون تبديلاً على $\mathbb{R}$:

(أ) $f_1 : \mathbb{R} \to \mathbb{R}$ ، $f_1(x) := x+1$

(ب) $f_2 : \mathbb{R} \to \mathbb{R}$ ، $f_2(x) := x^2$

(جـ) $f_3 : \mathbb{R} \to \mathbb{R}$ ، $f_3(x) := -x^3$

(د) $f_4 : \mathbb{R} \to \mathbb{R}$ ، $f_4(x) := e^x$

(هـ) $f_5 : \mathbb{R} \to \mathbb{R}$ ، $f_5(x) := x^3 - x^2 - 2x$

(١٧) عين أى العبارات الآتية يكون صحيحاً أو خاطئاً :

(أ) التبديل (permutation) هو راسم واحد لواحد (one – to – one)

(ب) الراسم يكون تبديلاً إذا كان وفقط إذا كان واحداً لواحد .

(جـ) أى راسم من مجموعة منتهية على (onto) نفسها يكون واحداً لواحد .

(د) كل زمرة جزئية من زمرة إبدالية تكون إبدالية .

(هـ) كل عنصر فى زمرة يولد زمرة جزئية دائرية "داخل" الزمرة .

(و) الزمرة المتماثلة $S_{10} (= \gamma_{10})$ تتكون من عشرة عناصر .

(ز) الزمرة المتماثلة S_3 دائرية .

(ح) كل زمرة تكون متشاكلة (أيزومورفية) مع زمرة تبديلات .

(١٨) اوجد عدد مولدات الزمر الدائرية من الرتب 6 ، 8 ، 12 ، 60 .

(١٩) اوجد عدد العناصر فى كل من الزمر الآتية :

(أ) الزمرة الجزئية الدائرية فى $\mathbb{Z}_{30}$ المتولدة من $\overline{25}$

(ب) الزمرة الجزئية الدائرية فى $\mathbb{Z}_{12}$ المتولدة من $\overline{30}$

(جـ) الزمرة الجزئية الدائرية $[i]$ فى الزمرة $(\mathbb{C} \setminus \{0\}, .)$

(د) الزمرة الجزئية الدائرية فى الزمرة $(\mathbb{C} \setminus \{0\}, .)$ والمتولدة من $(1+i)/\sqrt{2}$

(هـ) الزمرة الجزئية الدائرية فى الزمرة $(\mathbb{C} \setminus \{0\}, .)$ والمتولدة من $1 + i$

(٢٠) فى كل من الزمر الآتية اوجد جميع الزمر الجزئية :

(أ) $\mathbb{Z}_{12}$ (ب) $\mathbb{Z}_{36}$ (د) $\mathbb{Z}_8$

(٢١) عين أى التقريرين الآتيين يكون صحيحاً أو خاطئاً

(أ) كل زمرة إبدالية تكون دائرية .

(ب) كل عنصر فى زمرة دائرية يولد الزمرة

(٢٢) اضرب مثالاً مضاداً للتقرير الآتى : "إذا كانت كل زمرة جزئية فعلية من الزمرة G دائرية ، فإن G تكون دائرية" .

(٢٣) إذا كان p ، q عددين أوليين فاوجد عدد مولدات الزمرة الدائرية $\mathbb{Z}_{pq}$

(٢٤) ليكن p عدداً أولياً . كم عدد مولدات الزمرة الدائرية $\mathbb{Z}_{p^r}$ حيث $r \geq 1$ عدد صحيح

(٢٥)عين أى العبارات الآتية يكون صحيحاً أو خاطئاً :

(أ) كل زمرتين من الرتبة 3 تكونان متشاكلتين (أيزومورفيزميتين)

(ب) بدون حساب الأيزومورفيزمات هناك زمرة دائرية واحدة من رتبة منتهية .

(جـ) لايمكن أن يوجد أيزومورفيزم (تشاكل) بين زمرة جمعية (أى عمليتها هى الجمع) ، وزمرة ضربية (أى عمليتها هى الضرب)

(د) $(\mathbb{R},+)$ أيزومورفية مع زمرة تبديلات

(٢٦) لتكن $(G,.)$ زمرة . اعتبر العملية * المعرفة على المجموعة G كالآتى :

$$\forall a,b \in G: \qquad a*b := b.a$$

برهن على أن $(G,*)$ زمرة وهى متشاكلة (أيزومورفية) مع $(G,.)$

(ارشاد : اعتبر الراسم : $\begin{matrix} \varphi : G \to G \\ a \mapsto a^{-1} \end{matrix}$)

(٢٧) لتكن $(S,*)$ زمرة الأعداد الحقيقية فيما عدا -1 مع العملية * ، معرفة كالآتى : $a*b=a+b+ab$. برهن على أن $(S,*)$ متشاكلة مع $(\mathbb{R}\setminus\{0\},.)$ (عرف أيزومورفيزماً (تشاكلاً) $\psi : \mathbb{R}^* \to S$ $(R^* := \mathbb{R}\setminus\{0\})$)

(٢٨) بدون حساب الأيزومورفيزمات ، كم عدد الزمر ذات الرتبة 17 ؟

(٢٩) برهن على أن أى زمرة تحتوى على عنصرين على الأقل وليس لها زمر جزئية فعلية تكون منتهية ، ورتبتها عدد أولى

(٣٠) حدد إذا ما كانت التقارير الآتية صائبة أو خاطئة :

(أ) كل زمرة جزئية من أية زمرة لها مجموعة مشاركة يسرى

(ب) عدد المجموعات المشاركة اليسرى بالنسبة لزمرة جزئية من زمرة منتهية يقسم رتبة الزمرة

(جـ) كل زمرة ذات رتبة هى عدد أولى تكون إبدالية

(د) لايمكن الحصول على مجموعات مشاركة يسرى بالنسبة إلى زمرة جزئية منتهية فى زمرة غير منتهية

(هـ) فقط الزمر الجزئية فى الزمر المنتهية يكون لها مجموعات مشاركة يسرى

(و) الزمرة الجزئية فى زمرة هى مجموعة مشاركة يسرى بالنسبة إلى نفسها .

(ز) كل زمرة منتهية تحتوى على عنصر من كل رتبة تقسم رتبة الزمرة

(ح) كل زمرة دائرية منتهية تحتوى على عنصر من كل رتبة تقسم رتبة الزمرة

(٣١) إذا كانت G زمرة ذات رتبة منتهية ، وكانت H، K زمرتين جزئيتين فى G بحيث إن $H \subset K \subset G$ ، فبرهن على أن:

$$[G:H]=[G:K].[K:H]$$

(٣٢) أكمل الجمل الآتية :

(أ) زمرة القسمة $\mathbb{Z}_6 / [3]$ رتبتها ____

(ب) رتبة المجموعات المشاركة $[4] + 5$ فى زمرة القسمة $\mathbb{Z}_{12} / [4]$ هى ____

(جـ) رتبة المجموعة المشاركة $[12] + 26$ فى زمرة القسمة $\mathbb{Z}_{60} / [12]$ هى ____

(٣٣) حدد أى التقارير الآتية يكون صواباً وأيها يكون خطأ :

(أ) يمكن فقط أن يكون هناك معنى لزمرة القسمة G/N إذا كانت وفقط إذا كانت N زمرة جزئية طبيعية من G

(ب) كل زمرة جزئية من زمرة إبدالية G تكون زمرة جزئية طبيعية من G

(جـ) أى أوتومورفيزم داخلى لزمرة إبدالية يكون هو راسم الوحدة

(د) زمرة القسمة لزمرة منتهية تكون كذلك منتهية

(هـ) يقال لزمرة إنها <u>زمرة التواء</u> <u>**(torsion group)**</u> إذا كان كل عنصر فيها له رتبة منتهية . كل زمرة قسمة لزمرة التواء تكون كذلك زمرة التواء

(و) يقال لزمرة إنها **خالية من الالتواء** (**free torsion group**) إذا كانت رتب جميع عناصرها خلا العنصر المحايد غير منتهية

كل زمرة خالية من الالتواء تكون أى زمرة من زمر قسمتها خالية من الالتواء كذلك

(ز) كل زمرة قسمة لزمرة إبدالية تكون زمرة إبدالية

(ح) $\mathbb{R}/n\mathbb{R}$ زمرة دائرية رتبتها n حيث $n\mathbb{R}=\{nr|r\in\mathbb{R}\}$ ، $\mathbb{R}$ تحت عملية الجمع .

(٣٤) برهن على ان مجموعة جميع $g\in G$ (حيث G زمرة) بحيث إن $\varphi_g : G \to G$ هو أوتومورفيزم الوحدة الداخلى 1_e تكون زمرة جزئية طبيعية فى الزمرة G

(٣٥) احسب زمرة الإبداليات (الزمرة المشتقة) G' للزمرة D_4 (زمرة التماثلات على المربع) (انظر أمثلة ٤٤ ، ٤٥ ، ٤٨ من الأمثلة المتنوعة)

(٣٦) يقال لزمرة إنها **بسيطة**(**simple**) إذا لم تحتو من الزمر الجزئية الطبيعية إلا التافهة برهن على أنه إذا احتوت زمرة منتهية G على زمرة جزئية دليلها = ٢ فإن G لايمكن أن تكون بسيطة

(٣٧) برهن على أنه إذا كانت H ، N زمرتين جزئيتين فى زمرة G ، وكانت N زمرة جزئية طبيعية فى G فإن $H\cap N$ تكون طبيعية فى H . اعط مثالاً لبيان أن $H\cap N$ ليست بالضرورة طبيعية فى G

(٣٨) برهن على أنه إذا كانت N زمرة جزئية طبيعية فى G ، وكانت H زمرة جزئية فى G فإن $HN = NH$. وإذا كانت H كذلك زمرة جزئية طبيعية فى G فإن HN تكون زمرة جزئية طبيعية فى G .

(٣٩) هل هناك معنى للحديث عن أصغر زمرة جزئية طبيعية فى زمرة بحيث تحتوى على مجموعة من الزمرة ؟ ولماذا ؟

(٤٠)برهن على أن زمرة الأوتومورفيزمات الداخلية لزمرة G تكون زمرة جزئية طبيعية من زمرة الأوتومورفيزمات على G تحت عملية تحصيل الرواسم (انظر (١-٤-٤))

(٤١) برهن على أنه إذا كانت زمرة G منتهية تحتوى بالضبط على زمرة جزئية واحدة H من رتبة معينة فإن H تكون زمرة جزئية طبيعية فى G .

(٤٢) لتكن G زمرة تحتوى على الأقل على زمرة جزئية ذات رتبة منتهية s . برهن على أن تقاطع جميع الزمر الجزئية فى G من الرتبة s يكون زمرة جزئية طبيعية من G

(٤٣) برهن على أن الراسم $\begin{aligned}\varphi:(\mathbb{R},+)&\to(\mathbb{C}\setminus\{0\},.)\\ x&\mapsto\cos x+i\sin x\end{aligned}$ هومومورفيزم واوجد نواته

(٤٤) حدد أى التقارير الآتية يكون صحيحاً أو خاطئاً :

(أ) صورة زمرة مكونة من6 عناصر بواسطة هومومورفيزم ربما تتكون من 4 عناصر

(ب) صورة زمرة مكونة من6 عناصر بواسطة هومومورفيزم ربما تتكون من12 عنصراً

(جـ) يوجد هومومورفيزم من زمرة ذات 6 عناصر إلى زمرة ذات 12 عنصراً

(د) يوجد هومومورفيزم من زمرة ذات 6 عناصر إلى زمرة ذات 10 عناصر

(هـ) ليس من الممكن الحصول على هومومورفيزم من زمرة غير منتهية إلى زمرة منتهية

(و) يكون الهومومورفيزم أيزومورفيزماً (تشاكلاً) إذا اعتبرنا أن النطاق المصاحب هو الصورة ، وكانت النواة تتكون من العنصر المحايد فقط

(٤٥) لتكن G_1 ، G_2 زمرتين وليكن $\varphi_1:G_1\to G_2$ ، $\varphi_2:G_2\to G_1$ هومومورفيزمين بحيث إن $\varphi_2 o\varphi_1:G_1\to G_1$ ، $\varphi_1 o\varphi_2:G_2\to G_2$ راسما الوحدة . برهن على أن كلاً من φ_1 ، φ_2 أيزومورفيزم لـ G_1 ، G_2 ، وأن $\varphi_1=(\varphi_2)^{-1}$

(٤٦) لتكن G زمرة إبدالية منتهية لها الرتبة n ، وليكن r عدداً صحيحا موجباً ، ليس بينه وبين n قواسم مشتركة سوى 1 .

(أ) برهن على أن الراسم $\begin{aligned}\varphi:G&\to G\\ a&\mapsto a^r\end{aligned}$ هو أيزومورفيزم لـ G على نفسها

(ب) استنتج أن المعادلة $x^r=a$ لها حل وحيد دائماً فى الزمرة الإبدالية المنتهية G إذا لم يكن بين r، n قواسم مشتركة سوى 1 . ماذا يحدث إذا كان هناك قاسم مشترك بين r ، n غير 1 ؟

(٤٧) لتكن G ، G' زمرتين ، ولتكن H ، H' زمرتين جزئيتين طبيعيتين فى G ، G' على الترتيب . ليكن φ هومومورفيزماً من G إلى G' . برهن على أن φ يستحدث الهومومورفيزم الطبيعى $\varphi_*:G/H\to G'/H'$ إذا كان $\varphi(H)\subset H'$

(٤٨)اعتبر المجموعة $G=\{0,1,2,3,4,5,6,7\}$. لتكن G زمرة لها العملية * المعرفة كالآتى:

(أ) $a*b\le a+b$ $\qquad\forall a,b\in G:$

(ب) $a * a = 0$ $\forall a \in G:$

أنشئ جدول الزمرة (انظر ١-٢-٧)

(تسمى هذه الزمرة أحيانا **زمرة نيم** Nim)

(٤٩) لتكن F تعنى انعكاساً فى D_{10} ، R_α تعنى دوراناً بزاوية α . عبر عن العنصر $(R_{36}F)^{-1}$ كحاصل ضرب ، بدون استخدام أسس سالبة (انظر مثال ٤٨)

(٥٠) إذا كانت G زمرة منتهية فبرهن على أنه يوجد عدد فردى من العناصر $x \in G$ التى تحقق $x^3 = e$ ، وأنه يوجد عدد زوجى من العناصر $x \in G$ التى تحقق $x^2 \neq e$

(٥١) برهن على أن المجموعة { 35، 25، 15، 5} تحت عملية الضرب مقياس 40 تكون زمرة . ما عنصر الوحدة فيها ؟ هل هناك علاقة بينها وبين الزمرة $U(8)$ ؟

(٥٢) ليكن الجدول الآتى جدول زمرة . املأ الأماكن الخالية :

	e	a	b	c	d
e	e	_	_	_	_
a	_	b	_	_	e
b	_	c	d	e	_
c	_	d	_	a	b
d	_	_	_	_	_

(٥٣) العددان 5 ، 15 ضمن تجمع من 12 عدداً صحيحاً تكون جميعاً زمرة تحت عملية الضرب مقياس 56 . اوجد باقى الأعداد

(٥٤) برهن على أن الزمرة G إبدالية إذا كان وفقط إذا كان لكل $a,b \in G$:

$$(ab)^{-1} = a^{-1}b^{-1}$$

(٥٥) برهن على أن مجموعة الأعداد $3^m 6^n$ حيث $m,n \in \mathbb{Z}$ تكون زمرة تحت عملية الضرب

(٥٦) برهن على أن مجموعة المصفوفات من النوع 3×3 ذات العناصر من الأعداد الحقيقية والتى على الصورة :

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

تكون زمرة مع عملية الضرب المعرفة كالآتى :

$$\begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & a' & b'\\0 & 1 & c'\\0 & 0 & 1\end{bmatrix}=\begin{bmatrix}1 & a+a' & b'+ac'+b\\0 & 1 & c'+c\\0 & 0 & 1\end{bmatrix}$$

(تسمى هذه الزمرة **زمرة هايزنبرج** نسبة إلى عالم الفيزياء الألمانى فرنر هايزنبرج Werner Heisenberg صاحب جائزة نوبل للعلوم سنة ١٩٣٢، ولها علاقة وثيقة بمبدأ اللاحتمية لهايزنبرج فى ميكانيكا الكم (Heisenberg Uncertainty Principle of Quantum Physics)

(٥٧) برهن على أن $U(20)$ ليست دائرية

(٥٨) اوجد زمرة يتحقق لعنصرين فيها a ، b الآتى : $Ord(a)=Ord(b)=2$ بينما :

(أ) $Ord(ab)=3$ (ب) $Ord(ab)=4$ (جـ) $Ord(ab)=5$

هل توجد علاقة ما بين $Ord(a)$، $Ord(b)$، $Ord(ab)$ ؟

(٥٩) لتكن G زمرة. برهن على أن : $Z(G)=\bigcap_{a\in G} C(a)$ (انظر مثال ٥٤ من أمثلة متنوعة)

(٦٠) اوجد أصغر زمرة جزئية من $\mathbb{Z}$ تحتوى على :

(أ) 14، 8 (أى هى [14، 8]) (ب) 13، 8

(جـ) 15، 6 (د) m ، n

فى كل حالة اوجد عدد صحيحاً k بحيث تكون الزمرة الجزئية هى $[k]$

(٦١) لتكن $H:=\{x\in U(20)\,|\,x\equiv 1 \bmod 3\}$. هل H زمرة جزئية من $U(20)$ ؟

(٦٢) لأى عدد صحيح موجب n ولأية زاوية θ برهن على أنه فى زمرة المصفوفات من النوع 2×2 وعناصرها من $\mathbb{R}$ ومحددها = 1 يكون :

$$\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}^n=\begin{bmatrix}\cos n\theta & -\sin n\theta\\ \sin n\theta & \cos n\theta\end{bmatrix}$$

استخدم هذه الصيغة لحساب رتبة :

$$\begin{bmatrix} \cos\sqrt{2^0} & -\sin\sqrt{2^0} \\ \sin\sqrt{2^0} & \cos\sqrt{2^0} \end{bmatrix} \text{ ، } \begin{bmatrix} \cos 60^0 & -\sin 60^0 \\ \sin 60^0 & \cos 60^0 \end{bmatrix}$$

(هندسياً تمثل المصفوفة $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ دوراناً فى المستوى بزاوية θ)

(٦٣) $U(15)$ تحتوى على 6 زمر جزئية دائرية . اوجدها

(٦٤) D_4 تحتوى على 7 زمر جزئية دائرية . اوجدها . اوجد كذلك زمرة جزئية من D_4 رتبتها 4 تكون غير دائرية

(٦٥) لتكن H زمرة جزئية طبيعية من K ، K زمرة جزئية طبيعية من G . برهن أو انف : H زمرة جزئية طبيعية من G

(٦٦) اضرب مثالاً لزمرة غير إبدالية تكون كل زمرها الجزئية زمراً جزئية طبيعية

(٦٧)برهن بالاستقراء الرياضى على أنه إذا كان $H_i \lhd G, i=1,2,...,k$ فإن $H_1H_2...H_k \subset G$ زمرة جزئية . $(H_1H_2...H_k := \{h_1h_2...h_k \mid h_i \in H_i\})$ (تذكر أن $N \lhd G$ تعنى N زمرة جزئية طبيعية فى G)

(٦٨) فى المسألة السابقة مباشرة برهن أو انف : $H_1H_2...H_k \lhd G$ (انظر مثال٤٢ من أمثلة متنوعة)

(٦٩) احصل على صورة هومومورفية (homomorphic image) رتبتها 4 فى الزمرة الثمانية (مثال ٤٥ من أمثلة متنوعة)

(ارشاد : الزمرة الثمانية $H := \{e, \alpha^2\} \lhd G$ ، الصورة الهومومورفية هى G/H بواسطة الهومومورفيزم الطبيعى هى الصورة المنشودة)

(٧٠) إذا كان f أوتومورفيزماً للزمرة G بحيث إن $f(x) = x^{-1}$ لجميع $x \in G$ ، فبرهن على أن G إبدالية

(٧١) لتكن G زمرة إبدالية منتهية رتبتها n ، وليكن m عدداً صحيحاً موجباً ، $gcd\,(m,n) = 1$. برهن على أن الراسم $\begin{matrix} f: G \to G \\ x \mapsto x^m \end{matrix}$ أوتومورفيزم .

(٧٢) إذا كانت $G := S_3$ فبرهن على أن G تكون أيزومورفية (متشاكلة) مع زمرة الأوتومورفيزمات الداخلية لـــ G

(إرشاد : انظر مثال ٤٩ من أمثلة متنوعة)

(٧٣) إذا كان $Ord(a) = 30$ فكم عدد المجموعات المشاركة اليسرى لـــ $[a^4]$ فى $[a]$ ؟ اسرد هذه المجموعات .

(٧٤) اوجد زمرة غير منتهية تحتوى على زمرة جزئية منتهية .

(٧٥) برهن على أن الزمر الوحيدة التى لا تحتوى على زمر جزئية فعلية هى الزمر الدائرية التى رتبها أعداد أولية أو الزمرة التى تتكون من العنصر المحايد فقط .

(٧٦) إذا كانت A مجموعة جزئية ليست بالضرورة زمرة جزئية من الزمرة G ، فيمكن كذلك تعريف مطبع A كما سبق أن عرفنا فى حالة A زمرة جزئية من G. برهن على أنه إذا كانت A مجموعة جزئية من G فإن $Nor\,(A)$ يكون أيضاً زمرة جزئية من G . وبرهن كذلك على أنه إذا كانت A زمرة جزئية من G فإن $A \lhd G$ إذا كان وفقط إذا كان $N(A) = G$

(٧٧) برهن على أنه إذا كانت G متشاكلة مع H $(G \cong H)$ فإن $G' \cong H'$ ، $Z(G) \cong Z(H)$

(انظر مثالى ٤٩ ، ٥١ من أمثلة متنوعة)

(٧٨) ليكن لدينا $(\mathbb{Q} \setminus \{0\}, .)$ ، $N := \{-1, 1\}$. ولتكن H هى الزمرة المتولدة من $\{\frac{1}{2}\}$.

اوجد HN ، HN/N ومن ثم حقق النظرية الأولى للأيزومورفيزم $HN/N \cong H/H \cap N$

(٧٩) لتكن H، K زمرتين جزئيتين من G ، N زمرة جزئية طبيعية من G ، $HN = KN$. برهن على أن $H/H \cap N \cong K/K \cap N$

(٨٠) لتكن G زمرة ، $N_1 \lhd G$ ، $N_2 \lhd N_1$ ، ولتكن G/N_1 ، N_1/N_2 ، N_2 إبدالية .

ولتكن H زمرة جزئية من G . برهن على أنه توجد زمر جزئية H_1، H_2 من G بحيث يكون $H_1 \lhd H$ ، $H_2 \lhd H_1$ ، H/H_1 ، H_1/H_2 ، H_2 كلها إبدالية .

(٨١) فسر بطريقتين مختلفتين لماذا $\mathbb{Z}_4$ ليست متشاكلة مع زمرة كلاين الرباعية

(٨٢) لتكن G زمرة دائرية، ولها المولد a . وليكن $\varphi: G \to G'$ تشاكلاً (أيزومورفيزماً). برهن على أنه لأى $x \in G$ يكون $\varphi(x)$ متحدداً تماماً بـ $\varphi(a)$

(٨٣) عين عدد الأوتومورفيزمات لـ $\mathbb{Z}_2$ ، $\mathbb{Z}_6$ ، $\mathbb{Z}_8$ ، $\mathbb{Z}$ ، $\mathbb{Z}_{17}$

(إرشاد : استخدم التمرين ٨٢ السابق مباشرة)

(٨٤) لتكن G زمرة دائرية تتألف من n من العناصر ، وتتولد من a . ليكن $b = a^s \in G$. برهن على أن b يولد زمرة جزئية دائرية $H \subset G$ تتكون من $\frac{n}{d}$ عنصراً ، حيث d هو القاسم المشترك الأعظم لـ n ، s .

(٨٥) برهن على أن : $Aut(\mathbb{Z}_n) \cong U(n)$ لكل n عدد طبيعى موجب



Permutation Groups زمر التبديلات

٢-١ المفاهيم الأساسية

٢-١-١ تعريف : يقال لزمرة ما إنها زمرة تبديلات permutation group

إذا كانت زمرة جزئية من زمرة متماثلة

وكما جاء فى (١-٢-٥) فإن $\gamma(X)$ هى الزمرة المتماثلة على المجموعة غير الخالية X ، بينما γ_n هى الزمرة المتماثلة على مجموعة مكونة من n من العناصر . وقد ذكرنا من قبل أن كثيراً من المراجع تستخدم الرمز S_n بدلاً من γ_n .

٢-١-٢ نظرية كيلى Cayley's Theorem

كل زمرة تكون متشاكلة (أيزومورفية) مع زمرة تبديلات

البرهان : لتكن G زمرة

الراسم : $\forall a \in G: \quad \begin{matrix} \ell_a : G \to G \\ x \mapsto ax \end{matrix}$

هو النقل الأيسر (The left translation) حول a .

الراسم : $\begin{matrix} \ell : G \to \gamma(G) \\ a \mapsto \ell_a \end{matrix}$

هومومورفيزم (انظر (١-٣-٨) مثال٣)

$Ker(\ell) = \{a \in G : \ell_a = 1_G \in \gamma(G)\}$ (1_G هو راسم الوحدة على G)

$= \{a \in G : \ell_a(x) = 1_G(x) \ \ \forall x \in G\}$

$= \{a \in G : ax = x \ \ \forall x \in G\}$

$= \{e\}$ (e العنصر المحايد فى G)

$\Rightarrow$ ℓ inj راسم احادى

١-٣-٥ (أ)

ومن ثم فإن $\ell(G)$ تكون متشاكلة (أيزومورفية) مع زمرة جزئية من $\gamma(G)$.

٢-١-٣ نظرية : رتبة (γ_n) = $n!$ $(Ord(\gamma_n) =)$

البرهان : بالاستقراء الرياضى . سنبرهن هنا على أنه إذا كا لدينا مجموعتان A، B كل منهما تتكون من n من العناصر ، فإن عدد التناظرات الأحادية من A إلى B هو $n!$.

وسيكون الاستقراء على n .

عند $n = 1$: واضح أنه يوجد بالضبط تناظر أحادى واحد من A إلى B . نفترض أن الادعاء صحيح للمجموعتين اللتين تتكون كل منهما من $n - 1$ من العناصر .

والآن لتكن $A := \{a_1, ..., a_n\}$ ، $B := \{b_1, ..., b_n\}$. ولتكن $A_i := A \setminus \{a_i\}$ ، $B_i := B \setminus \{b_i\}$.

إذا كان φ تناظراً أحادياً من A إلى B بحيث إن $\varphi(a_n) = b_i$ فإن :

$$\varphi' : A_n \ni a \mapsto \varphi(a) \in B_i$$

سيكون تناظراً أحادياً من A_n إلى B_i . وبالعكس فإن كل تناظر أحادى $\varphi' : A_n \to B_i$ يمكن أن يمتد كالآتى :

$$\varphi(a) := \varphi'(a) , \qquad a \in A_n$$
$$\varphi(a_n) = b_i$$

فيصبح تناظراً أحاديا $\varphi : A \to B$. ومن فرض الاستقراء الرياضى يكون هناك $(n - 1)$! تناظراً أحادياً من A_n إلى B_i ، وبالتالى يكون هناك $(n - 1)$! تناظراً أحادياً من A إلى B بحيث إن $\varphi(a_n) = b_i$. ومن حيث إن هذا يتحقق لكل $i = 1, ..., n$ ، فإن عدد كل التناظرات الأحادية من A إلى B يكون $n(n - 1)! = n!$

<u>**٢-١-٤ تعريف**</u> : لتكن X مجموعة غير خالية ، $\gamma(X)$ هى الزمرة المتماثلة على X .

يسمى العنصر π فى $\gamma(X)$ <u>**دورة**</u> (cycle) (منتهية (finite)) ، عندما توجد عناصر عددها منته x_1، ...، x_m بحيث إن :

$$\pi(x_i) = x_{i+1} \quad \forall i \in \{1, ..., m-1\}, \pi(x_m) = x_1,$$
$$\pi(x) = x \qquad \forall x \in X \setminus \{x, ..., x_m\}$$

وسنكتب $\pi = (x_1, ..., x_m)$ ، ونسمى m <u>**طول**</u> (The length) <u>**الدورة**</u>. ويقال للدورة التى طولها 2 إنها <u>**نقلة**</u> أو <u>**تحويلة**</u> (transposition) ويقال لدورتين $(x_1, ..., x_m)$ ، $(y_1, ..., y_n)$ إنهما <u>**منفصلتان**</u> (disjoint) إذا كانت المجموعتان $\{x_1, ..., x_m\}$ ، $\{y_1, ..., y_n\}$ منفصلتين.

<u>**٢-١-٥ نظرية**</u> : كل تبديلة $\sigma \neq 1$ (1 هو عنصر الوحدة فى زمرة التبديلات) على مجموعة X تكون تركيباً $\gamma_1 ... \gamma_k$ من دورات منفصلة γ_i ، كل منها طوله 2 أو أكثر. وفيما عدا تغيير ترتيب هذه الدورات فإن σ لها تركيب وحيد .

<u>البرهان</u> : يعرف <u>**المسار**</u> C(orbit) لنقطة $x \in X$ تحت تأثير التبديلة σ بأنه المجموعة

$\{x,\sigma(x),\sigma^2(x),..\}$ لجميع صور x تحت تأثير القوى σ^i لـــ σ ومثل هذا المسار يكون منتهياً ، ولهذا سنصل حتماً إلى $\sigma^n(x)=\sigma^{n+k}(x)$ لعددين صحيحين مـــوجبين n ، k .
ومن ثم فبتطبيق σ^{-n} نحصل على : $\sigma^k(x)=x$ ، وإذا كان m أصغر عـــدد صـــحيح موجب بحيث يكون $\sigma^m(x)=x$ ، فإن المسار يتكون بالضبط من m من النقط المختلفـــة $C=\{x,\sigma(x),...,\sigma^{m-1}(x)\}$. وكذلك فإن كل نقطة $\sigma^i(x)$ فى هذه المجموعـــة C لهـــا نفس المسار (نفس النقط فى ترتيب دورى مختلف). التبديلة σ محددة على هذه المجموعة الجزئية $C\subset X$ هى تبديلة دورية $\sigma=(x\ \sigma(x)...\sigma^{m-1}(x))$ لها الطول m .
كل نقطة $x\in X$ تنتمى إلى مسار واحد بالضبط لـــ σ . ليكن هناك k من المسارات C_1، ... ، C_k لـــ σ ، و σ محددة على كل C_i هى تبديلة دورية γ_i . علاوة على هذا فإنه إذا كان $i\neq j$ فإن الدورتين γ_i ، γ_j تكونان منفصلتين .التركيب $\gamma_1...\gamma_k$ من هذه الدورات المنفصلة هو تبديلة على X ، لها نفس التأثير على نقطة $x\in X$ مثلما تفعل σ لأن $\sigma(x)$ هى $\gamma_i(x)$ إذا كانت x تنتمى إلى المسار C_i . ومن ثم فإن σ هى التركيب $\gamma_1...\gamma_k$ من الدورات المنفصلة . فى هذا التركيب أى دورة لها الطول 1 أى هى نقطة ثابتة يمكن أن تحذف .
وعلى الجانب الآخر فإنه لأى تركيب $\sigma=\beta_1...\beta_\ell$ لـــ σ فى صورة دورات منفصلة تكون "الحروف" المتحركة بدورة β_j أحد المسارات C_i لـــ σ ، ومن ثم فإن β_j هى الدورة المناظرة γ_i فى التركيب السابق $\gamma_1...\gamma_k$. ومن ثم فإن أى تركيبين يختلفان فقط فى ترتيب العوامل .

<u>**٢-١-٦استنتاج**</u>: رتبة أى تبديلة هى المضاعف المشترك الأصغر لأطوال دوراتها <u>**المنفصلة**</u> .

<u>**البرهان**</u> : فى التمثيل الدورى $\sigma=\gamma_1...\gamma_k$ الـــ $\gamma's$ تكون منفصلة ، وهكذا فإن $\gamma_i\gamma_j=\gamma_j\gamma_i$ ، ومن ثم فإنه لأى عدد صحيح m : $\sigma^m=\gamma_1^m...\gamma_k^m$ ومن ثم فإن $\sigma^m=1$ إذا كان وفقط إذا كان أى $(\gamma_i)^m=1$ ، ومن ثم إذا كان وفقط إذا كان m مضاعفاً مشتركاً لأطوال هذه الدورات γ_i . رتبة σ هى أصغر مثل هذه الـــ m . وهى النتيجة المطلوبة.
(قارن مع (١-١١-١))

٢-١-٧ تعريف : لتكن τ تبديلة فى الزمرة المتماثلة S_n . عندئذ فإن الراسم $\varphi : \sigma \mapsto \tau\sigma\tau^{-1}$ لكل $\sigma \in S_n$ يكون أوتومورفيزماً لـــ S_n لأن :

$$\varphi(\sigma_1\sigma_2) = \tau\sigma_1\sigma_2\tau^{-1} = \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1} = \varphi(\sigma_1)\varphi(\sigma_2)$$

أى أن φ هومومورفيزم . كذلك فإن الراسم العكسى لـــ φ هو

$$\psi : \sigma \mapsto \tau^{-1}\sigma\tau$$

لأن

$$\psi o \varphi(\sigma) = \psi(\varphi(\sigma)) = \psi(\tau\sigma\tau^{-1}) = \tau^{-1}\tau\sigma\tau^{-1}\tau = \sigma,$$

$$\varphi o \psi(\sigma) = \varphi(\psi(\sigma)) = \varphi(\tau^{-1}\sigma\tau) = \tau\tau^{-1}\sigma\tau\tau^{-1} = \sigma,$$

يسمى هذا الراسم (الأوتومورفيزم) **ترافق بـــ** τ (conjugate by τ) (انظر (١-٣-٧))

٢-١-٨ نظرية :

إذا كانت $\gamma \in S_n$ دورة لها الطول m فإن أى ترافق $\tau\gamma\tau^{-1}$ لـــ γ يكون له نفس الطول.

البرهان : إذا كانت γ هى الدورة $\gamma = (x_1, ..., x_m)$ فإننا سنبرهن على أن $\tau\gamma\tau^{-1}$ هى الدورة :

$$\tau(x_1\ x_2 ... x_m)\tau^{-1} = (\tau(x_1)\tau(x_2)...\tau(x_m)) \qquad (*)$$

لتكن $\tau\gamma\tau^{-1}$ مؤثرة على أى "حرف" y . كذلك فإن $y = \tau(\tau^{-1}(y))$. إذا كانت $x = \tau^{-1}(y)$ ليست واحدة من الـــ x_i's فإن التأثير $\tau\gamma\tau^{-1}$ على y يكون $\tau(x) \mapsto x \mapsto x \mapsto \tau(x)$ ، بينما إذا كانت $x = x_i$ فإن التأثير يكون كالآتى : $\tau(x_i) \mapsto x_i \mapsto x_{i+1} \mapsto \tau(x_{i+1})$.
وهذا بالضبط التأثير للدورة المكتوب فى الطرف الأيمن من (*) .

الترافق $\tau\gamma\tau^{-1}$ لأى تبديلة σ يمكن حسابه : اكتب σ كحاصل الضرب $\gamma_1 ... \gamma_k$ لدورات منفصلة . لأن كل ترافق هو أوتومورفيزم ، $\tau\sigma\tau^{-1} = (\tau\gamma_1\tau^{-1})...(\tau\gamma_k\tau^{-1})$ ، وكل دورة فى الطرف الأيمن يمكن التعبير عنها كما جاء فى (*) ، فهكذا يمكن حساب الترافق . بعبارة أخرى لكى نرافق σ لـــ τ ، نطبق الدالة τ على كل حرف فى تمثيل الدورات المنفصلة لـــ σ .

٢-١-٩ نظرية : أى تبديلة σ على {n ، ... ، 1} هى تركيبة من النقلات (التحويلات)

البرهان : نظراً لأن σ هى تركيبة $\gamma_1 ... \gamma_k$ من الدورات γ_i's ، يكفى أن نثبت المطلوب لدورة ، وذلك كالآتى :

$$(1\ 2\ \dots\ m) = (1\ m)\ \dots\ (1\ 3)\ (1\ 2)$$

والآن سنقسم التبديلات على$\{n$ ، ...،1$\}$ إلى قسمين: زوجى ، فردى . نعتبر المجموعة D المكونة من كل الأزواج المرتبة $\{1,...,n\}\times\{1,...,n\}\ni(i,j)$ حيث $i<j$ ، ونقول إن التبديلة $\sigma:\{1,...,n\}\to\{1,...,n\}$ تعكس الزوج $(i,j)\in D$ إذا كان $\sigma(i)>\sigma(j)$. ولتكن $\text{sgn}(\sigma)$ تشير إلى العدد الكلى لهذه الانعكاسات لـ σ ، ونسمى $(-1)^{\text{sgn}(\sigma)}$ __صنف__ σ ، ويقال إن σ __زوجية__ إذا كان $(-1)^{\text{sgn}(\sigma)}=+1$ ويقال إنها __فردية__ إذا كان $(-1)^{\text{sgn}(\sigma)}=-1$. بعبارة أخرى فإن σ تكون فردية إذا عكست عدداً فردياً من الأزواج المرتبة . وعلى سبيل المثال فإن صورة 6 5 4 3 بـ (6 3) هى 3 4 5 6 ، وهكذا فإن (6 3) عكست الأزواج المرتبة (4، 3) ، (5، 3) ، (3,6) ، (6، 4) ، (6، 5). وبصفة عامة فإن النقلة (التحويلة) ($h\ k$) حيث ($h<k$) تعكس الأزواج (h, k) وكل الأزواج (h, i) ، (i, k) حيث $h<i<k$ فقط . وبالتالى فإن أى __نقلة (تحويلة) تكون فردية__. لاحظ أن صنف σ هو $(-1)^{\text{sgn}(\sigma)}=\pm1$ عنصر من الزمرة الضربية (The multiplicative group) $\{+1, -1\}$ (الدائرية ذات الرتبة 2) .

__٢-١-١٠ نظرية__ : الراسم $\sigma\mapsto(-1)^{\text{sgn}(\sigma)}$ الذى يرسم كل تبديلة فى صنفها هو هومومورفيزم زمر $S_n\mapsto\{+1,-1\}$.

__البرهان__ : العدد $\text{sgn}(\sigma)$ يحدد عدد الأزواج (i , j) فى المجموعة D (مجموعة كل الأزواج (i , j) فى $\{n$ ، ...، 1$\}$) حيث $i<j$ ، التى تعكسها σ . هذا يتضمن تطبيق σ على المجموعة D للحصول على المجموعة $\sigma(D)$ لكل الأزواج $(\sigma(i),\sigma(j))$ حيث $i<j$. أيضاً لكل $k<\ell$ فى $\{n$ ، ...، 1$\}$ المجموعة $\sigma(D)$ يجب أن تحتوى على واحد بالضبط من الزوجين (k,ℓ) ، (ℓ,k) . والآن نطبق مرة أخرى التبديلة τ على $\sigma(D)$ لنحصل على المجموعة $\tau(\sigma(D))$ التى تحتوى إما على $(\tau(k),\tau(\ell))$ وإما على $(\tau(\ell),\tau(k))$. فى كلتا الحالتين هذا الزوج سينعكس بالضبط (من ترتيبه فى $\sigma(D)$) عندما ينعكس الزوج (k,ℓ) بـ τ . وهكذا فإن τ تعكس $\text{sgn}(\tau)$ من الأزواج فى $\sigma(D)$، بحيث إن المسار $D\to\sigma(D)\to\tau(\sigma(D))$ يعكس $\text{sgn}(\sigma)+\text{sgn}(\tau)$ من الأزواج . بعض هذه الأزواج ربما انعكس مرتين وهكذا عاد

إلى أصله . وعلى الجانب الآخر فإن المسار المباشر $D \to (\tau\sigma)(D)$ يعكس $\operatorname{sgn}(\tau\sigma)$ من الأزواج . ومن ثم فإنه بكتابة هذا مقياس 2 (modulo 2) لحساب الأزواج التى انعكست مرتين يكون لدينا :

$$\operatorname{sgn}(\tau\sigma) \equiv (\operatorname{sgn}(\tau) + \operatorname{sgn}(\sigma))(\operatorname{mod} 2)$$

وهذا يؤدى إلى :

$$(-1)^{\operatorname{sgn}(\tau\sigma)} = (-1)^{\operatorname{sgn}(\tau)}(-1)^{\operatorname{sgn}(\sigma)}$$

ومن ثم فإن $\sigma \mapsto (-1)^{\operatorname{sgn}(\sigma)}$ يكون هومومورفيزماً .

٢-١-١١ نتيجة :

حاصل ضرب k من النقلات يكون فردياً أو زوجيا حسب k فردى أو زوجى .

ونظراً لأن تبديلة σ يمكن أن تكتب بطرائق متعددة كحاصل ضرب نقلات (تحويلات) فإذا كان احد هذه التحليلات (factorizations) له عدد زوجى من النقلات فإن كل تحليل آخر يكون له عدد زوجى من النقلات .

وبالطبع فإن صنف أى تبديلة يمكن حسابه من تمثيل دوراته المنفصلة ، بمجرد معرفتنا صنف هذه الدورات .

٢-١-١٢ نتيجة : الدورة γ التى لها الطول m لها الصنف $(-1)^{\operatorname{sgn}(\gamma)} = (-1)^{m-1}$

البرهان: من النظرية (٢-١-٩) الدورة $(1\ 2 \ldots m)$ هى حاصل ضـــرب $m-1$ من النقـــلات $(1\ 2)\ (1\ 3) \ldots (1\ m)$ ، كل منها فردى .

٢-١-١٣ نتيجة : المجموعة $A_n(n > 1)$ ، مجموعة كل التبديلات الزوجية على $\{1، 2، \ldots، n\}$ هى زمرة جزئية من S_n وعدد عناصرها $\dfrac{n!}{2}$

(تسمى هذه الزمرة الزمرة المتغيرة (The alternating group) من الدرجة n

البرهان : نظراً لأن $\sigma \mapsto (-1)^{\operatorname{sgn}(\sigma)}$ هومومورفيزم فإن $\sigma \mapsto 1$ ، $\tau \mapsto 1$ يؤديان إلى $\sigma\tau \mapsto 1$. وهكذا فإن $A_n \subset S_n$ تكون مغلقة (closed) بالنسبة لعملية الضرب ومن ثم فبمثال ٤ من أمثلة متنوعة على الباب الأول تكون A_n زمرة جزئية من S_n . والآن لتكن عناصر A_n هى σ_1 ، ... ، ... ، σ_t ، اضرب كلاً منها فى تبديلة فردية مناسبة ، ولتكن $(1\ 2)$ تحصل على $\sigma_1(1\ 2)$، ... ، $\sigma_t(1\ 2)$ ، وكلها تبديلات فردية ، وكلها كذلك

مختلفة. ولكن كل تبديلة فردية ρ لها حاصل الضرب $\rho(1\ 2)=\sigma_i$ وهى زوجية ، وهكذا فإن $\rho=\sigma_i(1\ 2)$ وتكون ρ واحدة من المجموعة $\sigma_1(1\ 2)$ ، ... ، $\sigma_t(1\ 2)$. ونستنتج من هذا أن عدد التبديلات الفردية يساوى عدد التبديلات الزوجية يساوى نصف العدد الكلى $n\,!$ ، عدد التبديلات S_n .

٢-١-١٤ أمثلة محلولة :

مثال ١ : برهن على أنه إذا كانت α تبديلة معبراً عنها بعدد زوجى من النقلات أى كانت زوجية ، فإن كل تركيبة لـــ α من حاصل ضرب نقلات ستكون متكونة مـــن عدد زوجـــى من النقـــلات

(انظر (٢-١-١١)) .

البرهان : لتكن $\alpha=\beta_1\beta_2...\beta_r$ ، $\alpha=\gamma_1\gamma_2...\gamma_s$ حيث β_i's ، γ_j's كلها نقلات . والآن $\beta_1\beta_2...\beta_r=\gamma_1\gamma_2...\gamma_s$ يقتضى أن $1=\gamma_1\gamma_2...\gamma_s\beta_r^{-1}...\beta_2^{-1}\beta_1^{-1}$ حيث 1 هو تبديلة الوحدة وهى زوجية (لماذا ؟). ومن حيث إن $\beta_i^{-1}=\beta_i$ لجميع i فإن $r+s$ يكون عدداً زوجياً ، ومن ثم فإن r، s زوجيان معاً ، أو فرديان معاً .

مثال ٢ : برهن على الدورات المنفصلة تكون إبدالية .

البرهان: ليكن لدينا الدورتان المنفصلتان $\alpha=(a_1a_2...a_m)$ ، $\beta=(b_1b_2...b_n)$ من المجموعة

$$S=\{a_1,a_2,...,a_m,b_1,b_2,...,b_n,c_1,c_2,...,c_k\}$$

حيث الـــ $c's$ هى عناصر S التى تبقى ثابتة تحت تأثير α ، β . والآن حتى نبرهن على أن $\alpha\beta=\beta\alpha$ فإنه ينبغى لنا أن نبرهن على أن $(\alpha\beta)(x)=(\beta\alpha)(x)$ لجميع $x\in S$. والآن لتكن $x=a_i$ فإن :

$$(\alpha\beta)(a_i)=\alpha(\beta(a_i))=\alpha(a_i)=a_{i+1}$$ (a_{i+1} هو a_1 إذا كان $i=m$)

$$(\beta\alpha)(a_i)=\beta(\alpha(a_i))=\beta(a_{i+1})=a_{i+1}$$

أى أنه

$$\forall a_i:(\alpha\beta)(a_i)=(\beta\alpha)(a_i)$$

وبالمثل فإن

$$\forall b_i:(\alpha\beta)(b_i)=(\beta\alpha)(b_i)$$

والآن لتكن $x=c_i$:

$$(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i,$$
$$(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i$$

أى أن $\alpha\beta = \beta\alpha$ وهو المطلوب

مثال ٣ : عين إذا ما كانت التبديلات الآتية زوجية أو فردية

(١) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ (٢) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$

(٣) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 1 & 6 & 4 \end{pmatrix}$ (٤) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 2 & 6 & 7 & 5 \end{pmatrix}$

(٥) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 3 & 2 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 2 & 5 \end{pmatrix}$

الحل: (١) عدد الانعكاسات = 1 (2 سبق 1) + 1 (4 سبق 3)

= 2

التبديلة زوجية

(٢) عدد الانعكاسات = 4 (5 سبقت 3 ، 2 ، 4 ، 1) + 2 (3 سبقت 2 ، 1)

+1 (2 سبق 1) + 1 (4 سبق 1)

= 8

التبديلة زوجية

(٣) عدد الانعكاسات = 2 (3 سبقت 2 ، 1) + 3 (5 سبقت 2 ، 1 ، 4)

+1 (2 سبقت 1) + 0 + 1 (6 سبقت 4)

= 7

التبديلة فردية

(٤) عدد الانعكاسات = 3 (4 سبقت 3 ، 1 ، 2) + 2 (3 سبقت 1 ، 2)

+ 0 + 0 + 1 (6 سبقت 5)

+ 1(7 سبقت 5) = 7

التبديلة فردية

طريقة أخرى للأجزاء الأربعة الأولى :

(١) التبديلة هى : $\sigma=(12)(34)$ وهذه تبديلة زوجية لأن صنفها $(\operatorname{sgn}(\sigma))$ هو $(-1)^2$ أى 1

(٢) التبديلة هى : $(2\ 3)(1\ 5)$ ، كما فى (1) هى زوجية

(٣) التبديلة هى : $(1\ 3\ 2\ 5\ 6\ 4)$ وهذه يمكن كتابتها كالآتى :

$$(1\ 3\ 2\ 5\ 6\ 4) = (1\ 4)(1\ 6)(1\ 5)(1\ 2)(1\ 3)$$

وبهذا يكون صنفها $(-1)^5$ أى -1 ، أى هى فردية

كذلك يمكن التعبير عن التبديلة كالآتى

$(4\ 1\ 3\ 2\ 5\ 6)$ وبالتالى هى كذلك

$$(4\ 6)(4\ 5)(4\ 2)(4\ 3)(4\ 1)$$

وبالطبع هى فردية ، كما سبق

(٤) التبديلة هى :

$(1\ 4\ 2\ 3)(5\ 6\ 7)$. وهذه يمكن كتابتها كالآتى :

$(1\ 3)(1\ 2)(1\ 4)(5\ 7)(5\ 6)$ أو $(3\ 2)(3\ 4)(3\ 1)(5\ 7)(5\ 6)$

وهى فردية

(٥) التبديلة هى : $(1\ 3\ 4\ 6\ 5\ 2)(1\ 4\ 3\ 6\ 5\ 2)$ وهى :

$$(1\ 2)(1\ 5)(1\ 6)(1\ 4)(1\ 3)(1\ 2)(1\ 5)(1\ 6)(1\ 3)(1\ 4)$$

أى أن التبديلة زوجية .

<u>مثال ٤</u>: برهن على أن : $A_n = S_n \Rightarrow n=1$

(S_n ، A_n معرفتان كما سبق)

<u>البرهان</u> : إذا كانت $n > 1$ فإن S_n ينبغى لها أن تحتوى على تبديلة تبادل 1 ، 2 وتبقى كل "الحروف" الأخرى ثابتة . ومن ثم فإن هذه التبديلة تكون فردية ومن ثم فهى لا تنتمى إلى A_n ، وبالتالى فإن $A_n \neq S_n$. إذن حتى تكون $A_n = S_n$ يجب أن تكون $n=1$.

<u>مثال ٥</u> : عين رتبة كل من التبديلات الآتية :

(١) $(1\ 2\ 4)(3\ 5\ 7)$ (٢) $(1\ 2\ 4)(3\ 5\ 6)$

(٣) $(1\ 2\ 4)(3\ 5)$ (٤) $(1\ 2\ 4)(3\ 5\ 7\ 8)$

<u>الحل</u> : من (٢-١-٦) ينتج أن الرتب هى الآتية :

(1): 3 (2): 3 (3): $3 \times 2 = 6$ (4): $3 \times 4 = 12$

طريقة أخرى :

في حالة (4)

$$(1\ 2\ 4)\ (1\ 2\ 4) = (1\ 4\ 2)$$
$$(1\ 2\ 4)^3 = (1\ 2\ 4)(1\ 4\ 2) = 1$$

(1 راسم الوحدة على المجموعة {4، 2، 1})

$$(3\ 5\ 7\ 8)(3\ 5\ 7\ 8) = (3\ 7)(5\ 8)$$
$$(3\ 7)(5\ 8)(3\ 7)(5\ 8) = 1$$

1 راسم الوحدة على المجموعة {3, 5, 7, 8}

وبالتالي فإن رتبة التبديلة هي :

$$3 \times 4 = 12$$

<u>مثال ٦</u> : برهن على أن A_8 تحتوي على عنصر رتبته 15

<u>البرهان</u>: واضح أن هذا العنصر سيكتب على صورة حاصل ضرب دورتين منفصلتين إحداهما رتبتها (طولها) = 5 ، والأخرى رتبتها (طولها) = 3 . وينبغي أن تكون الدورتان زوجيتين معاً أو فرديتين معاً حتى يكون العنصر زوجياً فينتمي إلى A_8. الدورة $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ أو باختصار (3 2 1) زوجية لأن طولها (رتبتها) = 3 (٢-١-١١). الدورة $\begin{pmatrix} 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 4 \end{pmatrix}$ أو باختصار (8 7 6 5 4) زوجية لأن طولها (رتبتها) = 5

وحسب (٢-١-٦) تكون رتبة العنصر (8 7 6 5 4) (3 2 1) هي 15 .

<u>مثال ٧</u>: هل تكون التبديلات الفردية زمرة جزئية من S_n ؟ ولماذا ؟

<u>الحل</u> : العنصر المحايد $1 \in S_n$ زوجي لأن عدد انعكاساته = الصفر . ومن ثم فإن العنصر المحايد 1 لاينتمي إلى مجموعة التبديلات الفردية في S_n ، وبهذا لاتكون التبديلات الفردية زمرة جزئية من S_n.

<u>مثال ٨</u> : ليكن n عدداً صحيحاً موجباً. هل الدورة التي طولها n حيث n عدد فردي تكون زوجية أم فردية؟ وهل الدورة التي طولها n حيث n عدد زوجي تكون زوجية أم فردية ؟

<u>الحل</u> : n فردية : الدورة التي طولها n زوجية

n زوجية : الدورة التي طولها n فردية

(انظر (٢-١-١٢)) .

مثال ٩ : إذا كانت α تبديلة زوجية فبرهن على أن α^{-1} أيضاً تبديلة زوجية. وإذا كانت α تبديلة فردية فإن α^{-1} أيضاً تبديلة فردية .

البرهان : $1=\alpha^{-1}\alpha$ (تبديلة الوحدة) . من حيث إن عدد الانعكاسات فى 1 هو الصفر $\equiv$ (عدد الانعكاسات فى α + عدد الانعكاسات فى α^{-1}) (مقياس 2) (برهان (٢-١-١٠))
فإذا كان عدد الانعكاسات فى α زوجياً فكذلك يكون فى α^{-1} ، وإذا كان عدد الانعكاسات فى α فردياً فكذلك يكون عدد الانعكاسات فى α^{-1} .

مثال ١٠ : اوجد عنصرى زمرة α ، β بحيث يكون $Ord(\alpha)=3$ ، $Ord(\beta)=3$ ، $Ord(\alpha\beta)=5$.

الحل : $\alpha:=(1\ 2\ 3)$ ، $\beta:=(3\ 4\ 5)$.

$$(1\ 2\ 3)(3\ 4\ 5)=(3\ 4\ 5\ 1\ 2)$$

أى $(5\ \ 4\ \ 3\ \ 2\ \ 1)$ (انظر (١-٢-٥) مثال ٣)

مثال ١١ : لتكن H زمرة جزئية من S_n . برهن على أنه إما أن تكون كل عناصر H تبديلات زوجية أو أن نصف عناصر H بالضبط هى تبديلات زوجية .

البرهان : لتكن H تحتوى على تبديلة فردية σ ، ولتكن A هى مجموعة التبديلات الزوجية فى H، B هى مجموعة التبديلات الفردية فى H . واضح أن $\sigma A\subset B$. كذلك فإن عدد عناصر σA = عدد عناصر A ، ومن ثم فإن عدد عناصر A أقل من أو يساوى عدد عناصر B (*). وبالمثل فإن $\sigma B\subset A$ وعدد عناصر σB = عدد عناصر B ، ومن ثم فإن عدد عناصر B أقل من أو يساوى عدد عناصر A (*') . من (*) ، (*') ينتج أن عدد عناصر A = عدد عناصر B بافتراض وجود عنصر σ فردى .

مثال ١٢ : عبر عن التبديلة الآتية كحاصل ضرب دورات منفصلة

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 5 & 6 & 1 & 2 & 4\end{pmatrix}$$

الحـل :

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 5 & 6 & 1 & 2 & 4\end{pmatrix}=\begin{pmatrix}1 & 3 & 6 & 4\\ 3 & 6 & 4 & 1\end{pmatrix}\begin{pmatrix}2 & 5\\ 5 & 2\end{pmatrix}$$

مثال ١٣ : عبر من التركيبة الآتية كحاصل ضرب دورات منفصلة

$$(1\quad 2\quad 3)\,(3\quad 4\quad 5)\,(1\quad 3\quad 5)$$

الحـل :

$$(1\ 2\ 3)(3\ 4\ 5)(1\ 3\ 5) = (1\ 2\ 3)(1\ 4\ 5) = (1\ 4\ 5\ 2\ 3)$$

أو

$$(1\ 2\ 3)(3\ 4\ 5)(1\ 3\ 5) = (3\ 4\ 5\ 1\ 2)(1\ 3\ 5) = (1\ 4\ 5\ 2\ 3)$$

حصلنا على دورة واحدة وهى تحقق المطلوب .

مثال ١٤ : برهن على أن التبديلتين σ ، $\tau\sigma\tau^{-1}$ لهما نفس الصنف ، ولكن ليس بالضرورة نفس العدد من الا نعكاسات .

البرهان : من برهان (٢-١-١٠)

$$\begin{aligned}
\text{sgn}(\tau\sigma\tau^{-1}) &\equiv (\text{sgn}(\tau)+\text{sgn}(\sigma)+\text{sgn}(\tau^{-1})) \quad \text{mod}(2)\\
&= \quad (2\ \text{sgn}(\tau)+\text{sgn}(\sigma)) \quad \text{mod}(2)\\
&\equiv \text{sgn}(\sigma) \quad \text{mod}(2)
\end{aligned}$$

أى لهما نفس الصنف .

والآن خذ $\tau := (1\ 3\ 2)$ فيكون $\tau^{-1} := (1\ 2\ 3)$ ، $\sigma := (4\ 3\ 5)$. لإيجاد عدد الانعكاسات فى $\tau\sigma\tau^{-1}$:

$$\tau\sigma\tau^{-1} = (1\ 3\ 2)(4\ 3\ 5)(1\ 2\ 3) = (1)(3)(2\ 5\ 4) = (2\ 5\ 4)$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ 1 & 5 & 3 & 2 & 4\end{pmatrix}$$

ويكون عدد الانعكاسات هو :

$$3 + 1 = 4$$

بينما $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ 1 & 2 & 5 & 3 & 4\end{pmatrix}$ ويكون عدد الانعكاسات هو 2

مثال ١٥ : اوجد زمرة بها زمرتان جزئيتان مختلفتان لهما نفس الرتبة

الحـل : فى

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}(=(1\ \ 2)),\ \ \tau_2 = \begin{pmatrix} 1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}(=(1\ \ 3)):S_3(=\gamma_3)$$

$$Ord([\tau_1]) = 2 = Ord([\tau_2])$$

<u>مثال ١٦</u> : برهن على أن أى تبديلة رتبتها 14 على عشرة "حروف" تكون فردية .

<u>البرهان</u> : رتبة التبديلة = طولها . ومن حيث إن عـــدد حـــروف التبديلـــة 10 > 14 إذن لايمكن كتابة التبديلة كدورة واحدة. كذلك فمن (٢-١-٦) نستنتج أن التبديلة هى حاصـــل ضرب دورتين طول إحداهما 7 وطول الأخرى 2 فيكون من مثال 8 الدورة ذات الطـــول 7 زوجية ، والدورة (النقلة) ذات الطول 2 فردية، وتكون التبديلة فردية .

<u>مثال ١٧</u> : اختبر إذا ما كانت التبديلة الآتية زوجية أو فردية

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 6 & 5 & 1 & 7 & 2 \end{pmatrix}$$

<u>الحـــل</u> : يمكن التعبير عن σ كالآتى :

$$\begin{aligned} \sigma &= (1\ \ 4\ \ 5)(2\ \ 3\ \ 6\ \ 7) \\ &= (1\ \ 5)(1\ \ 4)(2\ \ 7)(2\ \ 6)(2\ \ 3) \end{aligned}$$

وبهذا تكون σ حاصل ضرب 5 نقلات ومن ثم فهى فردية .

<u>مثال ١٨</u> : برهن على أن أى عنصر فى A_n ، حيث $n > 3$ هو حاصل ضرب دورات طول كل منها 3 (A_n هو فى الواقع مجموعة كل حواصل ضرب الدورات التى طولها 3 من γ_n)

<u>البرهان</u> : لتكن $\sigma \in A_n$ ، حينئذ فإن σ تكون حاصل ضرب عدد زوجى من النقلات (التحويلات) التى يمكن "تجميعها" فى أزواج . ليكن (ab) ، (xy) زوجين مختلفين من النقلات . إذا كان (ab) ، (xy) منفصلتين فإن :

$$(ab)(xy) = (ab)((ax)(xa))(xy) = ((ab)(ax))((xa)(xy)) = (axb)(xya)$$

أما إذا كان (ab) ، (xy) غير منفصلتين، أى أن $\{a,b\} \cap \{x,y\} \neq \phi$ ، فليكن بدون أى فقدان للعمومية(without any loss of generality) ، $b=x$ وعندئذ فإن $(ab)(by)=(bya)=(aby)$ نهاية البرهان .

<u>مثال ١٩</u> : برهن على أن الزمرة المشتقة (زمرة الإبداليات) للزمرة $\gamma_n (= S_n)$ هى A_n إذا كانت $n \geq 2$.

<u>البرهان</u> : من نظرية لاجرانج نعلم أن $Ord(\gamma_n) = Ord(A_n).[\gamma_n : A_n]$

ومن ثم فإن : $Ord(\gamma_n / A_n) =: [\gamma_n : A_n] = \dfrac{Ord(\gamma_n)}{Ord(A_n)} \quad = \quad 2, \quad n \geq 2$

١٣-١-٢

وبالتالى فإن الزمرة γ_n / A_n دائرية لجميع $n \geq 2$ (١-١١- ٧) . وهى كذلك إبدالية (١-١١-٧). ومن مثال٥٣ من أمثلة متنوعة على الباب الأول ينتج أن (1) $\gamma'_n \subset A_n$ (= الزمرة المشتقة لـــ γ_n).

وواضح أن (2) $A_2 \subset \gamma'_2$. والآن إذا كانت $n \geq 3$ فمن مثال ١٨ كل عنصر فى A_n يمكن كتابته على صورة حاصل ضرب دورات طول كل منها 3 . وبالإضافة إلى هذا فإنه لكل $i, j, k \in \{1,...,n\}$ المختلفة

$$(ijk) = (i\ k)(jk)(ik)^{-1}(jk)^{-1} \in \gamma'_n, \quad n \geq 3$$

أى أن (3) $A_n \subset \gamma'_n$. من (1) ، (2) ، (3) ينتج أن $\gamma'_n = A_n, \; n \geq 2$.

مثال ٢٠ : برهن على أن الزمرة المشتقة لـــ A_n هى A_n إذا كانت $n \geq 5$

البرهان : واضح أن $A'_n \subset A_n$. يتبقى أن نثبت أنه لكل $n \geq 5$: $A_n \subset A'_n$ ومن مثال ١٨ أعلاه يكفى أن نثبت أنه لكل $n \geq 5$ ، كل دورة طولها 3 من γ_n ستكون إبدالياً من دورات طولها 3 من γ_n. ليكن $\alpha = (i\,j\,k)$ عنصراً فى γ_n ، وليكن $\ell, m \in \{1,...,n\}$ بحيث إن i، j، k، ℓ ، m كلها مختلفة $(n \geq 5)$ ضع $\pi := (i\,j\,\ell)$ ، $\sigma := (i\,k\,m)$ ينتج أن : $\pi\sigma\pi^{-1}\sigma^{-1} = \alpha$.

نهاية البرهان .

مثال ٢١ : ما أقل عدد من العناصر يكفى لتوليد S_3 ؟

الحـــل : يكفى العنصران (1 2) ، (1 3) لتوليد S_3 :

(1 3) (1 2) = (1 2 3) , (1 2) (1 3) = (1 3 2),
(1 2 3) (1 2 3) (1 2) = (2 3)

وبالطبع $(1\,2)^{٢} = e$ (العنصر المحايد)

مثال ٢٢ : برهن على أن S_n يمكن أن تتولد من المجموعة {(1 2), (1 2 3 … n)}

البرهان : سنبرهن أولاً على أن $(1\ 2\ 3\ ..\ n)^{n-r}(1\ 2)(1\ 2\ 3\ \dots\ n)^{r}$ يعطى جميع النقلات الآتية بتغيير r : (1 2) ، (2 3) ، (3 4) ، ... ، (n-1, n). ثم نبرهن على أن هذه

النقلات تولد جميع نقلات S_n . ومن النظرية (٢-١-٩) التى تنص على أن أى تبديلة هى تركيبة من النقلات يتم البرهان . والآن :

عند $r = 0$:

$$(1\ 2)\underbrace{(1\ 2\ 3\ \dots\ n)(1\ 2\ 3\ \dots\ n)\ \dots\ (1\ 2\ 3\ \dots\ n)}_{n \text{ من المرات}} = (1\ 2)$$

عند $r = 1$:

$$(1\ 2\ 3\ \dots\ n)(1\ 2)\underbrace{(1\ 2\ 3\ \dots\ n)(1\ 2\ 3\ \dots\ n)\ \dots\ (1\ 2\ 3\ \dots\ n)}_{n-1 \text{ من المرات}} = (2\ 3)$$

عند $r = n - 2$:

$$\underbrace{(1\ 2\ 3\ \dots\ n)(1\ 2\ 3\ \dots\ n)\ \dots\ (1\ 2\ 3\ \dots\ n)}_{n-2 \text{ من المرات}}(1\ 2)(1\ 2\ 3\ \dots\ n)(1\ 2\ 3\ \dots\ n) = (n-1,\ n)$$

عند $r = n - 1$:

$$\underbrace{(1\ 2\ 3\ \dots\ n)(1\ 2\ 3\ \dots\ n)\ \dots\ (1\ 2\ 3\ \dots\ n)}_{n-1 \text{ من المرات}}(1\ 2)(1\ 2\ 3\ \dots\ n) = (1\ n)$$

والآن نلاحظ أن : $(m\ k)\ (k\ n)\ (m\ k) = (m\ n)$

فإذا أردنا تكوين (3 7) – مثلاً – من النقلات السابقة سنجرى الآتى :

$$(3\ 5) = (3\ 4)\ (4\ 5)\ (3\ 4)$$
$$(3\ 6) = (3\ 5)\ (5\ 6)\ (3\ 5)$$
$$(3\ 7) = (3\ 6)\ (6\ 7)\ (3\ 6)$$

وبهذا يكون

$$\begin{aligned}(3\ 7) &= (3\ 5)(5\ 6)(3\ 5)(6\ 7)(3\ 5)(5\ 6)(3\ 5)\\ &= (3\ 4)(4\ 5)(3\ 4)(5\ 6)(3\ 4)(4\ 5)(3\ 4)(6\ 7)(3\ 4)(4\ 5)(3\ 4)(5\ 6)\\ &\quad (3\ 4)(4\ 5)(3\ 4)\end{aligned}$$

وعلى هذا المنوال يتم البرهان.

مثال ٢٣ : من مثال ٢٢ يتضح أن S_n يمكن أن تتولد من عنصرين ، ومن نظرية كيلى (٢-١-٢) كل زمرة منتهية تكون متشاكلة (أيزومورفية) مع زمرة تبديلات . إذن كل زمرة منتهية يمكن أن تتولد من عنصرين .

ما وجه الخطأ فى الاستنتاج السابق ؟

الحــل: وجه الخطأ أنه ليس كل زمرة جزئية من S_n يمكن أن تتولد من عنصرين وإنما S_n جميعها التى تتولد من عنصرين !

وكمثال على خطأ المقولة انظر مثال ١٨ فى ٤-١-١٢ (أمثلة متنوعة)

تمارين

(١) عبر عن التبديليتين الآتيتين كحاصل ضرب دورات منفصلة :

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 1 & 5 & 3 & 4 & 2\end{pmatrix},\ \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 6 & 4 & 5 & 7 & 3 & 1 & 2\end{pmatrix}$$

(٢) عبر عن التبديلات الآتية كحاصل ضرب دورات منفصلة :

$$(1\ \ 2\ \ 3\ \ 4\ \ 5)(1\ \ 5\ \ 6)(2\ \ 4\ \ 6),$$
$$(1\ \ 2\ \ 3\ \ 4)(2\ \ 3\ \ 4\ \ 5)(3\ \ 4\ \ 5\ \ 1),$$
$$(1\ \ 2)(2\ \ 3)(3\ \ 4)(4\ \ 5)(5\ \ 1)$$

(٣) اوجد أربع زمر جزئية مختلفة من S_4 تكون أيزومورفية (متشاكلة) مع S_3 ، تسعاً متشاكلة مع S_2 .

(٤) برهن على أنه يوجد على الأقل 30 زمرة جزئية مختلفة من S_6 متشاكلة مع S_3 .

(٥) برهن على أن S_n تتولد من النقلات : $(1\ 2)$ ، $(2\ 3)$ ، ... ، $(n-1, n)$.

(٦) عين رتبة كل من التبديلات الآتية :

$(1\ \ 5)$ ، $(1\ \ 2\ \ 3)$ ، $(2\ \ 3\ \ 6\ \ 7)$ ، $(a_1a_2...a_k)$

$(1\ \ 5\ \ 7)(4\ \ 3\ \ 8)$ ، $(1\ \ 2\ \ 4\ \ 8)(3\ \ 5\ \ 7)$ ، $(1\ \ 3\ \ 5\ \ 7\ \ 9\ \ 11)(2\ \ 4\ \ 6)$

(٧) عين رتبة التبديلتين الآتيتين :

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 1 & 5 & 4 & 6 & 3\end{pmatrix},\ \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 7 & 6 & 1 & 2 & 3 & 4 & 5\end{pmatrix}$$

(٨) ما الرتب المحتملة لعناصر : $S_6(=\gamma_6)$ ، S_7 ، A_6 ، A_7 ؟

(٩) عين أكبر رتبة لعناصر A_{10}

(١٠) عين صنف التبديلات الآتية :

$(1\ 2\ 4)$ ، $(1\ 4\ 6\ 8)$ ، $(1\ 2\ 4\ 5\ 7)$ ، $(1\ 3)(1\ 4\ 5)(2\ 5\ 7)$

$(1\ 2\ 4\ 7)(2\ 3\ 5\ 8)$

(١١) برهن على أن حاصل ضرب تبديلتين إحداهما زوجية والأخرى فردية هى تبديلة فردية .

(١٢) إذا كان $\alpha=\begin{pmatrix}1&2&3&4&5&6\\2&1&3&5&4&6\end{pmatrix}$ ، $\beta=\begin{pmatrix}1&2&3&4&5&6\\6&1&2&4&3&5\end{pmatrix}$

فاحسب : α^{-1} ، β^{-1} ، $\alpha o \beta$ ، $\beta o \alpha$

(١٣) لتكن $\alpha, \beta \in S_n$. برهن على أن $\alpha^{-1}\beta^{-1}\alpha\beta$ تكون تبديلة زوجية (المقصود بـــ $\alpha\beta$ هو $\alpha o \beta$ كما سبق) .

(١٤) برهن على أن : $(1\ 2\ 3)^{-1} = (3\ 2\ 1)$ ، $(1\ 4\ 7\ 8)^{-1} = (8\ 7\ 4\ 1)$ ،

$(a_n a_{n-1} \ldots a_2 a_1)^{-1} = (a_1 a_2 \ldots a_{n-1} a_n)$

(١٥) فى S_3 أوجد عنصرين α ، β بحيث يكون $Ord(\alpha)=2$ ، $Ord(\beta)=2$ ، $Ord(\alpha\beta)=3$.

(١٦) برهن على أنه إذا كانت G هى مجموعة التبديلات على الأعداد الصحيحة الموجبة، وكانت H هى المجموعة الجزئية من G التى يمكن التعبير عن عناصرها فى صورة حاصل ضرب أعداد منتهية من الدورات فإن H تكون زمرة جزئية من G .

(١٧) برهن على أن $Ord(A_n')=1$ إذا كانت $n \in \{2,3\}$.

(١٨) برهن على أن A_4' هى زمرة كلاين الرباعية .

1 Group Theory نظرية الزمر

القسم

الباب

3

حواصل الضرب الخارجية والداخلية المباشرة

External and Internal Direct Products

٣-١ حواصل الضرب الخارجية المباشرة

٣-١-١ تعريف : لتكن G_1 ، G_2 ، ... ، G_n زمراً . يعرف **حاصل الضرب الخارجي المباشر** لـ G_1 ، G_2 ، ... ، G_2 (The external direct product) ونشير إليه بالرمز $G_1 \otimes G_2 \otimes ... \otimes G_n$ بأنه المجموعة

$$G_1 \otimes G_2 \otimes ... \otimes G_n := \{(g_1, g_2, ..., g_n) \mid g_i \in G_i\}$$

حيث يعرف "الضرب" فى جاصل الضرب المباشر كالآتى:

$$(g_1, g_2, ..., g_n)(g_1', g_2', ..., g_n') := (g_1g_1', g_2g_2', ..., g_ng_n')$$

حيث يتم g_ig_i' حسب قانون الضرب فى الزمرة G_i .

ويمكن بسهولة البرهنة على أن حاصل الضرب الخارجى المباشر لمجموعة من الزمر هو زمرة . فحسب الرموز السابقة يكون العنصر المحايد فيه هو $(e_1, e_2, ..., e_n)$ حيث $e_i \in G_i$ هو عنصرها المحايد ، وحيث يكون معكوس $(g_1, g_2, ..., g_n)$ هو $(g_1^{-1}, g_2^{-1}, ..., g_n^{-1})$ حيث g_i^{-1} هو معكوس g_i .

٣-١-٢ تعريف : لتكن G_1 ، G_2 زمرتين $\varphi : G_2 \to Aut(G_1)$ هومومورفيزم زمر .

نعرف : لجميع $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$:

$$(x_1, x_2)(y_1, y_2) := (x_1\varphi(x_2)(y_1), x_2y_2)$$

٣-١-٣ ملحوظة : $G_1 \times G_2$ حيث G_1 ، G_2 زمرتان ، والعملية المعرفة فى (٣-١-٢) تكون زمرة .

البرهان:

$$\forall (x_1, x_2), (y_1, y_2), (z_1, z_2) \in G_1 \times G_2 :$$

$$((x_1, x_2)(y_1, y_2))(z_1, z_2) = (x_1\varphi(x_2)(y_1), x_2y_2)(z_1, z_2)$$

$$= (x_1\varphi(x_2)(y_1)\varphi(x_2y_2)(z_1), x_2y_2z_2) \qquad (1)$$

$$(x_1, x_2)((y_1, y_2)(z_1, z_2)) = (x_1, x_2)(y_1\varphi(y_2)(z_1), y_2z_2)$$

$$= (x_1\varphi(x_2)(y_1\varphi(y_2)(z_1)), x_2y_2z_2)$$

$$= (x_1\varphi(x_2)(y_1)\varphi(x_2)(\varphi(y_2)(z_1)), x_2y_2z_2)$$

$$= (x_1\varphi(x_2)(y_1)(\varphi(x_2) o \varphi(y_2))(z_1), x_2y_2z_2)$$

$$= (x_1\varphi(x_2)(y_1)\varphi(x_2y_2)(z_1), x_2y_2z_2) \qquad (2)$$

من (1) ، (2) ينتج أن

$$((x_1,x_2)(y_1,y_2))(z_1,z_2) = (x_1,x_2)((y_1,y_2)(z_1,z_2))$$

(e_1,e_2) هو العنصر المحايد للزمرة حيث $e_1 \in G_1$ ، $e_2 \in G_2$ العنصران المحايدان للزمرتين G_1 ، G_2 ، لأن :

$$\forall (x_1,x_2) \in (G_1 \times G_2 : (e_1,e_2)(x_1,x_2) = (e_1\varphi(e_2)(x_1), e_2x_2)$$

$$= (e_1 1_{G_1}(x_1), e_2x_2) = (e_1x_1, e_2x_2) = (x_1,x_2)$$

(1_{G_1} هو راسم الوحدة على G_1 وهو عنصر الوحدة فى $Aut(G_1)$)

معكوس العنصر $(x_1,x_2) \in G_1 \times G_2$ هو العنصر $(\varphi(x_2^{-1})(x_1^{-1}), x_2^{-1})$ لأن :

$$(\varphi(x_2^{-1})(x_1^{-1}), x_2^{-1})(x_1,x_2) = (\varphi(x_2^{-1})(x_1^{-1})\varphi(x_2^{-1})(x_1), x_2^{-1}x_2)$$

$$= (\varphi(x_2^{-1})(x_1^{-1}x_1), x_2^{-1}x_2) = (\varphi(x_2^{-1})(e_1), e_2) = (e_1,e_2)$$

تسمى هذه الزمرة شبه حاصل الضرب الخارجى المباشر لـ G_1 ، G_2 **بالنسبة إلى** φ

(The semi-external direct product of G_1 , G_2, w.r.t. φ)

ويرمز لها بالرمز $G_1 \times_\varphi G_2$

٣-١-٤ ملحوظة : واضح أن حاصل الضرب المباشر للزمرتين G_1 ، G_2 سيكون مساوياً لشبه حاصل الضرب المباشر لهما إذا كان الهومومورفيزم $\varphi : G_2 \to Aut(G_1)$ يحقق $\varphi(x_2) = 1_{G_1}$ لجميع $x_2 \in G_2$.

٣-١-٥ ملحوظة : G_1 ، G_2 زمرتان ، $e_1 \in G_1$ ، $e_2 \in G_2$ العنصران المحايدان .

$G_1 \times \{e_2\}$ ، $\{e_1\} \times G_2$ زمرتان جزئيتان من $G_1 \times_\varphi G_2$.

البرهان : بالنسبة إلى $\{e_1\}\times G_2$:

$$\forall a,b\in G_2 : (e_1,a)(e_1,b)=(e_1\varphi(a)(e_1),ab)=(e_1e_1,ab)=(e_1,ab)\in\{e_1\}\times G_2$$

كذلك فإن $(e_1,e_2)\in\{e_1\}\times G_2$. ولكل $a\in G_2$: معكوس العنصر $(e_1,a)\in\{e_1\}\times G_2$ هو : $(\varphi(a^{-1})(e_1^{-1}),a^{-1})$ وهو يساوى $(\varphi(a^{-1})(e_1),a^{-1})$ أى هو (e_1,a^{-1}) وهو عنصر فى $\{e_1\}\times G_2$ وبالنسبة إلى $G_1\times\{e_2\}$:

$$\forall a,b\in G_1 : (a,e_2)(b,e_2)=(a\varphi(e_2)b,e_2e_2)=(a1_{G_1}(b),e_2e_2)$$

$$=(ab,e_2)\in G_1\times\{e_2\}$$

كذلك فإن $(e_1,e_2)\in G_1\times\{e_1\}$. **ولكل** $a\in G_1$ معكوس العنصر $(a,e_2)\in G_1\times\{e_2\}$ هو $(\varphi(e_2^{-1})(a^{-1}),e_2^{-1})$ أى هو $(\varphi(e_2)(a^{-1}),e_2)$ أى هو $(1_{G_1}(a^{-1}),e_2)$ أى هو (a^{-1},e_2) وهو عنصر فى $G_1\times\{e_2\}$.

<u>٣-١-٦ مثال</u> : ليكن $G_1=G_2=(\mathbb{R},+)$ ، وليكن $\varphi:\mathbb{R}\to Aut(\mathbb{R})$ معرفة كالآتى :

$$\forall x,y\in\mathbb{R} : \varphi(x)(y)=e^xy$$

φ هومومورفيزم لأن :

$$\forall x_1,x_2,y\in\mathbb{R} : \varphi(x_1+x_2)(y)=e^{x_1+x_2}y=e^{x_1}e^{x_2}y$$

$$=\varphi(x_1)\varphi(x_2)(y)$$

لكل $(a,0)\in\mathbb{R}\times_\varphi\mathbb{R}$ ولكل $(0,x)\in\{0\}\times\mathbb{R}=H$

$$(a,0)+(0,x)=(a+\varphi(0)(0),0+x)=(a,x)$$

أى أن $\{a\}\times\mathbb{R}$ مجموعة مشاركة يسرى من $(a, 0)$ بالنسبة إلى H . كذلك فإن :

$$(0,x)+(a,0)=(0+\varphi(x)(a),x+0)$$

$$=(ae^x,x)$$

أى أن $\{(ae^x,x):x\in\mathbb{R}\}$ مجموعة مشاركة يمنى من $(a, 0)$ بالنسبة إلى H .

٣-١-٧ نظرية : رتبة عنصر فى حاصل الضرب المباشر لزمر منتهية هى المضاعف المشترك الأصغر (The least common multiple) لرتب "مركبات" العنصر . بالرموز :

$$Ord(g_1,g_2,...,g_n)=\ell cm\{Ord(g_1),Ord(g_2),...,Ord(g_n)\}$$

البرهان : ليكن $s=\ell cm\{Ord(g_1),...,Ord(g_n)\}$ ، $t=Ord(g_1,...,g_n)$

واضح أن :

$$(g_1,...,g_n)^s=(g_1^s,...g_n^s)=(e,...,e),$$

ومن (١-١١-٩) (١) فإن t يقسم s ، وعلى درجة الخصوص فإن: $t\le s$. كذلك فإن :

$$(g_1^t,...,g_n^t)=(g_1,...,g_n)^t=(e,...,e)$$

ومن ثم فمن (١-١١-٩) (١) كذلك فإن $Ord(g_1)$ ، ... ، $Ord(g_n)$ كلها تقسم t .

وهكذا فإن t هو مضاعف مشترك (common multiple) لرتبة g_1 ، ... ، ورتبة g_n ، وبالتالى فإن $s\le t$ لأن s هو المضاعف المشترك الاصغر لرتبة g_1 ، ... ، g_n . ومن (*) يكون $s=t$.

٣-١-٨ تمهيدية : إذا كان a ، b عددين صحيحين موجبين فإن :

$$ab=\ell cm\{a,b\}gcd\{a,b\}$$

البرهان : ليكن $a:=p_1^{m_1}...p_k^{m_k}$ ، $b:=p_1^{n_1}...p_k^{n_k}$ (يمكن استخدام 0 كأس عند الضرورة) ، حيث p_1 ، ... ، p_k أعداد أولية مختلفة ، m_1 ، ... ، m_k ، n_1 ، ... ، n_k أعداد صحيحة ليست سالبة . عندئذ فإن

$$\left.\begin{aligned}\ell cm\{a,b\}&=p_1^{s_1}...p_k^{s_k},s_i:=\max(m_i,n_i);\\ gcd\{a,b\}&=p_1^{t_1}...p_k^{t_k},t_i:=\min(m_i,n_i)\end{aligned}\right\rangle$$

$$\ell cm\{a,b\}gcd\{a,b\}=p_1^{m_1+n_1}...p_k^{m_k+n_k}=ab$$

٣-١-٩ نظرية : ليكن G ، H زمرتين دائريتين منتهيتين . عندئذ فإن $G\otimes H$ زمرة دائرية إذا كان وفقط إذا كان $Ord(G)$ ، $Ord(H)$ ليس لهما قواسم مشتركة (ماعدا ± 1)

<u>البرهان</u> : ليكن $Ord(G) = m$ ، $Ord(H) = n$ بحيث إن $Ord(G \otimes H) = mn$

"$\Rightarrow$": ليكن $G = [g]$ ، $H = [h]$. وليكن $gcd(m,n) = 1$ (القاسم المشترك الأعظم) أى أن m ، n ليس لهما قواسم مشتركة . عندئذ فإن :

$$Ord(g,h) = \ell cm\{m,n\} = mn = Ord(G \otimes H)$$

أى أن (g,h) مولد لـــ $G \otimes H$ ، أى أن $G \otimes H$ دائرية .

"$\Leftarrow$" : لتكن $G \otimes H$ دائرية والمطلوب إثبات أن m ، n ليس لهما قواسم مشتركة . لأن $G \otimes H$ دائرية فإنه يوجد عنصر (g,h) فى $G \otimes H$ رتبته mn . ومن النظرية (٣-١-٧) نحصل على :

$$mn = Ord(g,h) = \ell cm\{Ord(g), Ord(h)\}.$$

ومن جهة أخرى فلأن $Ord(g)$ تقسم m ، وكذلك $Ord(h)$ تقسم n (١-١٠-٣) ، ينتج أن $\ell cm\{Ord(g), Ord(h)\}$ يقسم $\ell cm\{m,n\}$. ولكن $\ell cm\{m,n\} \leq mn$ ، فينتج أن $\ell cm\{m,n\} = mn$ ، ومن ثم فإن $gcd\{m,n\} = 1$ أى أن m ، n ليس لهما قواسم مشتركة (٣-١-٨).

<u>٣-١-١٠ نتيجة</u> : حاصل الضرب الخارجى المباشر $G_1 \otimes G_2 \otimes ... \otimes G_n$ للزمر الدائرية المنتهية G_1 ، G_2 ، ... ، G_n يكون زمرة دائرية إذا كان وفقط إذا كان

$$gcd\{Ord(G_i), Ord(G_j)\} = 1, \quad i \neq j$$

<u>البرهان</u>: (٣-١-٩) مع الاستقراء الرياضى .

<u>٣-١-١١ نتيجة</u> : لتكن $m = n_1 n_2 ... n_k$ حيث n_1 ، n_2 ، ... ، n_k أعداد صحيحة موجبة . $\mathbb{Z}_m (= \mathbb{Z}/m\mathbb{Z})$ تكون متشاكلة (أيزومورفية) مع $\mathbb{Z}_{n_1} \otimes \mathbb{Z}_{n_2} \otimes ... \otimes \mathbb{Z}_{n_k}$ إذا كان وفقط إذا كان $gcd\{n_i, n_j\} = 1, \quad i \neq j$.

<u>البرهان</u> : (٣-١-٩) مع الاستقراء الرياضى .

<u>٣-١-١٢ نتيجة</u> : يمكن التعبير عن نفس الزمرة بطرائق مختلفة : فمثلاً :

$$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_6 \otimes \mathbb{Z}_5 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_{30},$$
$$\mathbb{Z}_2 \otimes \mathbb{Z}_6 \otimes \mathbb{Z}_5 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_5 \cong \mathbb{Z}_6 \otimes \mathbb{Z}_{10}$$

ومن ثم فإن : $\mathbb{Z}_2 \otimes \mathbb{Z}_{30} \cong \mathbb{Z}_6 \otimes \mathbb{Z}_{10}$ لكن $\mathbb{Z}_2 \otimes \mathbb{Z}_{30} \not\cong \mathbb{Z}_{60}$

٣-١-١٣ أمثلة محلولة :

مثال ١ : لتكن $U(n)$ هى زمرة كل الأعداد الصحيحة الموجبة التى أصغر من n ، والقاسم المشترك الأعلى (الأعظم) لها مع n هو 1 حيث يكون "الضرب" مقياس n

احسب $U(6) \otimes U(8)$.

الحـل : $U(6) = \{1,5\}$ ، $U(8) = \{1,3,5,7\}$ ومن ثم فإن :

$$U(6) \otimes U(8) = \{(1,1),(1,3),(1,5),(1,7),(5,1),(5,3),(5,5),(5,7)\}$$

لاحظ أن $(5, 3)(5, 5) = (1, 7)$ لأن $5.5 = 1 \pmod 6$ ، $3.5 = 7 \pmod 8$.

مثال ٢ : برهن على أن $\mathbb{Z}_2 \otimes \mathbb{Z}_3 \cong \mathbb{Z}_6$

البرهان : (انظر النظرية (٣-١-٩)) : من حيث أن $\mathbb{Z}_2$ ، $\mathbb{Z}_3$ دائريتان ، $gcd\{2,3\} = 1$ تكون $\mathbb{Z}_2 \otimes \mathbb{Z}_3 \cong \mathbb{Z}_6$.

وللتحقق من هذا حسابياً :

$$\mathbb{Z}_2 \otimes \mathbb{Z}_3 = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{0}),(\bar{1},\bar{1}),(\bar{1},\bar{2})\}$$

نجرب $(\bar{1},\bar{1})$ كمولد :

$$2(\bar{1},\bar{1}) = (\bar{2},\bar{2}) = (\bar{0},\bar{2}), 3(\bar{1},\bar{1}) = (\bar{3},\bar{3}) = (\bar{1},\bar{0}), 4(\bar{1},\bar{1}) = (\bar{4},\bar{4}) = (\bar{0},\bar{1}),$$
$$5(\bar{1},\bar{1}) = (\bar{5},\bar{5}) = (\bar{1},\bar{2}), 6(\bar{1},\bar{1}) = (\bar{0},\bar{0})$$

إذن $\mathbb{Z}_2 \otimes \mathbb{Z}_3$ دائرية يولدها $(\bar{1},\bar{1})$. عدد عناصرها 6 وتكون متشاكلة (أيزومورفية) مع $\mathbb{Z}_6$

طريقة أخرى مباشرة : باستخدام النتيجة (٣-١-١١)

مثال ٣ : برهن على $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ لها 7 زمر جزئية من الرتبة 2 .

<u>البرهان</u> :

$$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 = \{(\bar{0},\bar{0},\bar{0}),(\bar{0},\bar{0},\bar{1}),(\bar{0},\bar{1},\bar{0}),(\bar{0},\bar{1},\bar{1}), (\bar{1},\bar{0},\bar{0}),(\bar{1},\bar{0},\bar{1}),(\bar{1},\bar{1},\bar{0}),(\bar{1},\bar{1},\bar{1})\}$$

$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ تتكون من 8 عناصر ، أى مجموعة مكونة من $(\bar{0},\bar{0},\bar{0})$ مع عنصر آخر من العناصر السبعة الباقية تكون زمرة جزئية من $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$.

<u>مثال ٤</u> : برهن أو انف $\mathbb{Z} \otimes \mathbb{Z}$ زمرة دائرية .

<u>الحـل</u> : $\mathbb{Z} \otimes \mathbb{Z}$ ليس زمرة دائرية . لتكن $\mathbb{Z} \otimes \mathbb{Z}$ دائرية ومولدها (m, n) عندئذ فإنه يوجد عددان صحيحان k ، ℓ بحيث إن :

$(km, \ell n) = (1,1)$. وهذا يقتضى أن $m,n = \pm 1$. ولكن (m, n) لايمكن أن يولد $(-1, 2)$. إذن $\mathbb{Z} \otimes \mathbb{Z}$ ليست دائرية .

<u>مثال ٥</u> : هل $\mathbb{Z}_2 \otimes \mathbb{Z}_8 \cong \mathbb{Z}_{16}$ ؟ ولماذا ؟

<u>الحـل</u> : (انظر النظرية (٣-١-٩)) $\mathbb{Z}_2 \otimes \mathbb{Z}_8$ لايمكن أن تكون دائرية لأن $gcd\ \{2, 8\} = 2$ أما $\mathbb{Z}_{16}$ فهى دائرية (يولدها مثلاً $\bar{1}$ أى $1+16\mathbb{Z}$) ولايمكن أن يوجد أيزومورفيزم بينهما على الرغم من تساويهما فى الرتبة .

(انظر مثال ٨ من أمثلة متنوعة على الباب الأول)

طريقة أخرى : مباشرة من النتيجة (٣-١-١١) ينتج المطلوب .

<u>مثال ٦</u> : كم عدد العناصر فى $\mathbb{Z}_3 \otimes \mathbb{Z}_9$ التى من الرتبة 9 ؟

<u>الحـل</u> : (انظر النظرية (٣-١-٧)) .

سنحسب عدد العناصر (a, b) فى $\mathbb{Z}_3 \otimes \mathbb{Z}_9$ التى تحقق

$$9 = Ord(a,b) = \ell cm\{Ord(a), Ord(b)\}$$

وهذا يقتضى أن :

(i) $Ord(a) = 1, \qquad Ord(b) = 9$

أو

(ii) $Ord(a) = 3, \qquad Ord(b) = 9$

فى الحالة (i) يكون لـــ a إمكانية واحدة ولـــ b ست إمكانات فتكون b هى : $\bar{1}$ أو $\bar{2}$ أو $\bar{4}$ أو $\bar{5}$ أو $\bar{7}$ أو $\bar{8}$ وانظر الاستنتاج (١-١١-١١)) وبهذا تكون هناك 6 إمكانات للعنصر (a, b) .

فى الحالة (ii) يكون لـــ a إمكانتان ويكون لـــ b ست إمكانات ، وبهذا تكون هناك 12 من الإمكانات .

ويكون عدد العناصر فى $\mathbb{Z}_3 \otimes \mathbb{Z}_9$ التى لها الرتبة 9 هو 18 .

مثال ٧ : أوجد عدد العناصر التى لها الرتبة 4 فى $\mathbb{Z}_{8000000} \otimes \mathbb{Z}_{4000000}$

الحـــل : كما فى مثال ٦ السابق مباشرة سنحسب عدد العناصر (a,b) فى $\mathbb{Z}_{8000000} \otimes \mathbb{Z}_{4000000}$ التى تحقق

$$4 = Ord(a,b) = \ell cm\{Ord(a), Ord(b)\}$$

الإمكانات هى :

(i) $Ord(a) = 4$, $Ord(b) = 1$

وهنا يكون لـــ b إمكانية واحدة ، ولـــ a إمكانتان

فيكون $b = \bar{0}$ ، $a = \overline{2000000}$ أو $a = \overline{6000000}$

(ii) $Ord(a) = 4$, $Ord(b) = 2$

وهنا يكون لـــ b إمكانية واحدة ، a إمكانتان

فيكون $b = \overline{2000000}$ ، $a = \overline{2000000}$ أو $a = \overline{6000000}$

(iii) $Ord(a) = 4$, $Ord(b) = 4$

فيكون لكل من a ، b إمكانتان

فيكون $b = \overline{1000000}$ أو $b = \overline{3000000}$ ويكون $a = \overline{2000000}$ أو $a = \overline{6000000}$

(iv) $Ord(a) = 2$, $Ord(b) = 4$

فيكون لـــ a إمكانية واحدة ، لـــ b إمكانتان

فيكون $b = \overline{1000000}$ أو $b = \overline{3000000}$ ويكون $a = \overline{4000000}$

(v) $Ord(a) = 1, Ord(b) = 4$

فيكون لـــ a إمكانية واحدة ، لـــ b إمكانتان

فيكون $b=\overline{1000000}$ أو $b=\overline{3000000}$ ويكون $a=\overline{0}$

وبهذا يكون عدد العناصر التى لها الرتبة 4 هو :

$2+2+4+2+2=12$

مثال ٨ : لتكن G زمرة ولتكن $H:=\{(g,g)\,|\,g\in G\}$. برهن على أن H زمرة جزئية من $G\otimes G$ (تسمى هذه الزمرة قطر (The diagonal) $G\otimes G$). وإذا كانت $G=(\mathbb{R},+)$ فصف هندسيا $G\otimes G$ ، H .

الحـــل : $(e,e)\in H$ أى أن $H\neq\phi$

كذلك فلكل $(g,g),(h,h)\in H$:

$$(g,g)(h,h)^{-1}=(g,g)(h^{-1},h^{-1})=(gh^{-1},gh^{-1})\in H$$

أى أن H زمرة جزئية من $G\otimes G$.

والآن إذا كانت $G=\mathbb{R}$ فواضح أن $G\otimes G$ هى كل المستوى ، أما H فهى الخط المستقيم الذى معادلته $y=x$

مثال ٩ : برهن على أنه لأى زمرتين G_1 ، G_2 :

$$G_1\otimes G_2\cong G_2\otimes G_1$$

البرهان : نعرف

$$\varphi:G_1\otimes G_2\to G_2\otimes G_1$$
$$(x,y)\mapsto(y,x)$$

واضح أن φ تناظر أحادى .

φ هومومورفيزم لأن :

$$\forall(x,y),(x',y')\in G_1\otimes G_2:\varphi((x,y)(x',y'))=\varphi(xx',yy')=(yy',xx')$$
$$=(y,x)(y',x')=\varphi(x,y)\varphi(x',y')$$

أى أن φ أيزومورفيزم .

مثال ١٠ : ليكن G ، H زمرتين . برهن على أن G تشاكل (أيزومورفية مع) زمرة جزئية من $G \otimes H$

البرهان : ليكن e هو العنصر المحايد فى H . سنبرهن أولاً على أن $G \otimes \{e\}$ زمرة جزئية من $G \otimes H$ كالآتى : واضح أن $G \otimes \{e\}$ ليس مجموعة خالية فهو يحتوى على الأقل (e',e) حيث e' هو عنصر G المحايد . ولكل $(g,e),(h,e) \in G \otimes \{e\}$:

$$(g,e)(h,e)^{-1} = (g,e)(h^{-1},e) = (gh^{-1},e) \in G \otimes \{e\}$$

والآن نبرهن على أن : $G \cong G \otimes \{e\}$ كالآتى :

نعرف
$$\begin{aligned} \varphi : G &\to G \otimes \{e\} \\ g &\mapsto (g,e) \end{aligned}$$

واضح أن φ تناظر أحادى . كذلك φ هومومورفيزم لأن :

$$\forall g,h \in G : \varphi(gh) = (gh,e) = (g,e)(h,e) = \varphi(g)\varphi(h)$$

أى أن φ أيزومورفيزم . نهاية البرهان .

مثال ١١ : لتكن G زمرة إبدالية ، n عدداً صحيحاً موجباً . لتكن $G^n := \{g^n \mid g \in G\}$. برهن على أن G^n زمرة جزئية من G . والآن إذا كانت K ، H زمرتين إبداليتين فبرهن على أن $(H \otimes K)^n = H^n \otimes K^n$

البرهان : $e \in G^n$ العنصر المحايد أى أن G^n ليست مجموعة خالية . والآن

G^n زمرة جزئية من $G \Rightarrow$ $\forall g^n,h^n \in G^n : g^n(h^n)^{-1} = g^n(h^{-1})^n \underset{\text{إبدالية } G}{=} (gh^{-1})^n \in G^n$

والآن من حيث إن H ، K زمرتان إبداليتان فإن H^n ، K^n زمرتان جزئيتان من H ، K على الترتيب ، أى هما زمرتان . كذلك $H \otimes K$ إبدالية لأن H ، K إبداليتان (برهن على صحة ذلك) ومن ثم فإن $(H \otimes K)^n$ زمرة . والآن نبرهن على أن $(H \otimes K)^n = H^n \otimes K^n$ كالآتى :

$$(H\otimes K)^n \ni (h,k)^n = \underbrace{(h,k)...(h,k)}_{n \text{ من المرات}} = (h^n,k^n)\in H^n\otimes K^n$$

مثال ١٢ : برهن على أن $G\otimes H$ زمرة إبدالية إذا كان وفقط إذا كان G ، H زمرتين إبداليتين

البرهان : ليكن G ، H زمرتين إبداليتين . لكل $(g_1,h_1),(g_2,h_2)\in G\otimes H$:

$$(g_1,h_1)(g_2,h_2)=(g_1g_2,h_2h_2) \underset{G \text{ ، } H \text{ إبداليتان}}{=} (g_2g_1,h_2h_1)=(g_2,h_2)(g_1,h_1)$$

أى أن $G\otimes H$ إبدالية .

والآن وبدون فقد للعمومية(without any loss of generality)لتكن G ليست إبدالية ، أى أنه يوجد $g_1,g_2\in G$ بحيث يكون $g_1g_2\neq g_2g_1$. والآن ليكن $(g_1,h_1),(g_2,h_2)\in G\otimes H$. لدينا :

$$(g_1,h_1)(g_2,h_2)=(g_1g_2,h_1h_2)\neq(g_2g_1,h_2h_1)=(g_2,h_2)(g_1,h_1)$$

أى أن $G\otimes H$ ليست إبدالية .

(هذا المثال يجيب عن التساؤل فى مثال ١١ السابق مباشرة)

مثال ١٣ : لتكن $G:=\{3^m6^n/m,n\in\mathbb{Z}\}$ مع عملية الضرب العادية . برهن على أن G تتشاكل (أيزومورفية) مع $\mathbb{Z}\otimes\mathbb{Z}$

البرهان : سنعرف φ كالآتى :

$$\varphi: G\to\mathbb{Z}\otimes\mathbb{Z}$$
$$3^m6^n\mapsto(m,n)$$

واضح أن φ تناظر أحادى . φ هومورفيزم لأن :

$$\forall 3^{m_1}6^{n_1}\in G, 3^{m_2}6^{n_2}\in G:$$
$$\varphi(3^{m_1}6^{n_1}.3^{m_2}6^{n_2})=\varphi(3^{m_1+m_2}6^{n_1+n_2})=(m_1+m_2,n_1+n_2)$$
$$=(m_1,n_1)+(m_2,n_2)=\varphi(3^{m_1}6^{n_1})+\varphi(3^{m_2}6^{n_2})\Rightarrow\varphi \text{ أيزومورفيزم}$$

(تذكر أن العملية فى $\mathbb{Z}\otimes\mathbb{Z}$ هى الجمع)

مثال ١٤ : لتكن G زمرة من الرتبة 4 ، لجميع $x\in G$: $x^2=e$ حيث e عنصر G المحايد . برهن على أن $G\cong \mathbb{Z}_2\otimes\mathbb{Z}_2$

(تذكر أن $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$)

البرهان :

$$\mathbb{Z}_2\otimes\mathbb{Z}_2 := \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}, G:=\{e,x,y,z\}$$

سنضع جدولى "الضرب" لكل من G ، $\mathbb{Z}_2\otimes\mathbb{Z}_2$ ومنه يتضح التشاكل :

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

$+$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$

واضح أن $\varphi: Z_2\otimes\mathbb{Z}_2 \to G$ المعرف كالآتى :

$\varphi(\bar{0},\bar{0}) := e$ (العنصر المحايد فى G) ، $\varphi(\bar{0},\bar{1}) := x,$

$\varphi(\bar{1},\bar{0}) := y$ ، $\varphi(\bar{1},\bar{1}) := z$

أيزومورفيزم

مثال ١٥ : احسب الزمرة العاملة $\mathbb{Z}_4\otimes\mathbb{Z}_6/[(\bar{0},\bar{1})]$ (تذكر أن $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$)

الحـــل : $[(\bar{0},\bar{1})]$ هى زمرة جزئية دائرية من الزمرة $\mathbb{Z}_4\otimes\mathbb{Z}_6$ ، وهكذا فإن :

$$[(\bar{0},\bar{1})] = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{0},\bar{3}),(\bar{0},\bar{4}),(\bar{0},\bar{5})\}$$

$\mathbb{Z}_4\otimes\mathbb{Z}_6$ بها 24 عنصراً ، $[(\bar{0},\bar{1})]$ تتكون من 6 عناصر ، ومن ثم فإنه من نظرية لاجرانج ينتج أن : $\mathbb{Z}_4\otimes\mathbb{Z}_6/[(\bar{0},\bar{1})]$ تتكون من 4 عناصر ، وهى على وجه التحديد :

$$(\bar{0},\bar{0})+[(\bar{0},\bar{1})];(\bar{1},\bar{0})+[(\bar{0},\bar{1})];(\bar{2},\bar{0})+[(\bar{0},\bar{1})];(\bar{3},\bar{0})+[(\bar{0},\bar{1})]$$

مثال ١٦ : برهن على أن : $\mathbb{Z}_4 \otimes \mathbb{Z}_6 /[(\bar{0},\bar{2})] \cong \mathbb{Z}_4 \otimes \mathbb{Z}_2$

البرهان : $[(\bar{0},\bar{2})]$ هى زمرة جزئية دائرية من الزمرة $\mathbb{Z}_4 \otimes \mathbb{Z}_6$ ، وهى :

$$[(\bar{0},\bar{2})] = \{(\bar{0},\bar{0}),(\bar{0},\bar{2}),(\bar{0},\bar{4})\}$$

لاحظ أن $\bar{2}+\bar{2}+\bar{2}=\bar{6}=\bar{0}$ ، وهكذا فإن العامل الثانى $\mathbb{Z}_6$ "يطوى" بزمرة جزئية من الرتبة 3 ، ونحصل على زمرة عاملة من الرتبة 2 تكون متشاكلة مع $\mathbb{Z}_2$. العامل الأول يبقى كما هو $\mathbb{Z}_4$ وبهذا نصل إلى المطلوب .

مثال ١٧ : برهن على أن : $\mathbb{Z}_4 \otimes \mathbb{Z}_6 /[(\bar{2},\bar{3})] \cong \mathbb{Z}_4 \otimes \mathbb{Z}_3$

البرهان : لاحظ أن $[(\bar{2},\bar{3})] = \{(\bar{0},\bar{0}),(\bar{2},\bar{3})\}$

(لأن $[(\bar{2},\bar{3})]$ زمرة جزئية دائرية من $\mathbb{Z}_4 \otimes \mathbb{Z}_6$)

ورتبة $[(\bar{2},\bar{3})]$ هى 2 ، بينما رتبة $\mathbb{Z}_4 \otimes \mathbb{Z}_6$ هى 24 ، وبالتالى فإن $\mathbb{Z}_4 \otimes \mathbb{Z}_6 /[(\bar{2},\bar{3})]$ لها الرتبة 12 .

الزمر الإبدالية الممكنة من الرتبة 12 هى $\mathbb{Z}_4 \otimes \mathbb{Z}_3$ ، $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3$. $\mathbb{Z}_4 \otimes \mathbb{Z}_3$ لها عنصر من الرتبة 4 بينما $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3$ ليس لها مثل هذا العنصر . وواضح أن المجموعة المشاركة $(\bar{1},\bar{0})+[(\bar{2},\bar{3})]$ لها الرتبة 4 فى زمرة القسمة $\mathbb{Z}_4 \otimes \mathbb{Z}_6 /[(\bar{2},\bar{3})]$:

$$(\bar{1},\bar{0})+[(\bar{2},\bar{3})]+(\bar{1},\bar{0})+[(\bar{2},\bar{3})]+(\bar{1},\bar{0})+[(\bar{2},\bar{3})]+(\bar{1},\bar{0})+[(\bar{2},\bar{3})]$$
$$=(\bar{0},\bar{0})+[(\bar{2},\bar{3})]=[(\bar{2},\bar{3})]$$

وواضح أن لايمكن إضافة $(\bar{1},\bar{0})+[(\bar{2},\bar{3})]$ إلى نفسه عدداً أقل من المرات للحصول على $[(\bar{2},\bar{3})]$. ومعنى هذا أن $\mathbb{Z}_4 \otimes \mathbb{Z}_6 /[(\bar{2},\bar{3})]$ يحتوى على عنصر من الرتبة 4 ، وبهذا ينتج المطلوب

مثال ١٨ : اوجد أكبر رتبة لعنصر فى : (أ) $\mathbb{Z}_{12} \otimes \mathbb{Z}_{15}$ (ب) $\mathbb{Z}_6 \otimes \mathbb{Z}_8$

الحل : (أ) أكبر رتبة : $\ell cm\{12,15\} = 60$ المضاعف المشترك الأصغر

(ب) أكبر رتبة : $\ell cm\{6,8\} = 24$

(انظر نظرية (٣-١-٧))

مثال ١٩ : إذا كان كل عنصر لايساوى e العنصر المحايد فى زمرة منتهية G له الرتبة 2 ، فبرهن على أن رتبة G هى 2^n وأن $G=C_1\otimes C_2\otimes...\otimes C_n$ حيث $Ord(C_i) = 2$ ، (C_i دائرية)

البرهان : من مثال ١ فى أمثلة متنوعة على الباب الأول هذه الزمرة إبدالية .

والآن: ليكن $e\neq a_1\in G$. إما أن $G=[a_1]$ أى أن G دائرية ومولدها هو a_1 أو أن $[a_1]\subsetneq G$.

إذا كانت $G=[a_1]$ تكون هذه هى النهاية ! وإذا كانت $[a_1]\subsetneq G$ فإنه يوجد : $a_2 \in G$

بحيث إن $a_2 \notin [a_1]$. نكون حاصل الضرب الخارجى المباشر $[a_1]\otimes[a_2]$.

إما أن يكون $G=[a_1]\otimes[a_2]$ أو أن يكون $[a_1]\otimes[a_2]\subsetneq G$. فى الحالة الأولى نكون قد انتهينا . فى الحالة الثانية يوجد $a_3\in G$ ، $a_3 \notin [a_1]\otimes[a_2]$ ، ... وهكذا ... ولأن G منتهية فإننا نصل إلى $G=[a_1]\otimes[a_2]\otimes...\otimes[a_n]$ ، وكل $[a_i]$ زمرة دائرية لها الرتبة 2 .

مثال ٢٠ : برهن على أن أى زمرة G من الرتبة 4 إما أن تكون متشاكلة مع $\mathbb{Z}_4$ أو متشاكلة مع $\mathbb{Z}_2\otimes\mathbb{Z}_2$

البرهان : الزمرة G إما أن تكون دائرية فهى متشاكلة مع $\mathbb{Z}_4$ ، أو ليست دائرية . إذا لم تكن دائرية فهى تحتوى على زمر جزئية فعلية ، ومن نظرية لاجرانج رتبة الزمرة الجزئية تقسم رتبة الزمرة . إذن الزمرة الجزئية من G رتبتها 2 وتكون متشاكلة مع $\mathbb{Z}_2$ ويقتضى هذا أن تكون $G\cong\mathbb{Z}_2\otimes\mathbb{Z}_2$ (لأن رتبة G هى 4).

مثال ٢١ : برهن على أنه لايوجد إبيمورفيزم من $\mathbb{Z}_8\otimes\mathbb{Z}_2$ على $\mathbb{Z}_4\otimes\mathbb{Z}_4$.

البرهان : ليكن $\varphi:\mathbb{Z}_8\otimes\mathbb{Z}_2\to\mathbb{Z}_4\otimes\mathbb{Z}_4$ إبيمورفيزم . نطبق نظرية الهومومورفيزم (١-٨-١) فينتج أن : $\mathbb{Z}_4\otimes\mathbb{Z}_4\cong{}^{\mathbb{Z}_8\otimes\mathbb{Z}_2}/_{Ker(\varphi)}$. ومن ثم فإن

$Ord(\mathbb{Z}_4\otimes\mathbb{Z}_4)=Ord({}^{\mathbb{Z}_8\otimes\mathbb{Z}_2}/_{Ker(\varphi)})=16$ ومن نظرية لاجرانج (١-١٠-٣) ينتج أن

$Ord(\mathbb{Z}_8\otimes\mathbb{Z}_2)=Ord({}^{\mathbb{Z}_8\otimes\mathbb{Z}_2}/_{Ker(\varphi)}).Ord(Ker(\varphi))$ ومنها $Ord(Ker(\varphi))=1$

أى أن $Ker(\varphi)=\{(\bar{0},\bar{0})\}$ ، ويكون φ مونومورفيزم .

إذن φ أيزومورفيزم . لكن $\mathbb{Z}_8\otimes\mathbb{Z}_2$ بها عنصر رتبته 8 .

بينما $\mathbb{Z}_4\otimes\mathbb{Z}_4$ ليس بها عنصر رتبته8 ، وهذا تناقض. إذن لايوجد الإبيمورفيزم المفترض.

مثال ٢٢ : برهن على أن الراسم $\begin{matrix}\varphi:G\otimes H\to G\\(g,h)\mapsto g\end{matrix}$ حيث G، H زمرتان ، هومومورفيزم.

ما نواة (φ) ؟ يسمى هذا الراسم **إسقاط** (projection) $G\otimes H$ على G .

الحـــل :

$\forall(g_1,h_1),(g_2,h_2)\in G\otimes H:$

$$\varphi((g_1,h_1)(g_2,h_2))=\varphi(g_1g_2,h_1h_2)=g_1g_2=\varphi(g_1,h_1)\varphi(g_2,h_2)\Rightarrow\varphi$$ هومومورفيزم

$$Ker(\varphi)=\{(g,h)\in G\otimes H:g=e_G\ \ (\text{عنصر } G \text{ المحايد})\}$$

$$=\{(e_G,h)\in G\otimes H\}=\{e_G\}\otimes H$$

مثال ٢٣ : برهن على أن الراسم $\begin{matrix}\varphi:\mathbb{Z}\otimes\mathbb{Z}\to\mathbb{Z}\\(a,b)\mapsto a-b\end{matrix}$ هومومورفيزم . مانواة (φ) ؟

صف $\varphi^{-1}(3)$.

الحـــل :

$\forall(a,b),(c,d)\in\mathbb{Z}\otimes\mathbb{Z}:$

$$\varphi((a,b)+(c,d))=\varphi(a+c,b+d)=a+c-b-d=a-b+c-d$$

$= \varphi(a,b) + \varphi(c,d) \Rightarrow$ هومومورفيزم φ

$$Ker(\varphi) = \{(a,b) \in \mathbb{Z} \otimes \mathbb{Z} : \varphi(a,b) = a - b = 0\}$$
$$= \{(a,b) \in \mathbb{Z} \otimes \mathbb{Z} : a = b\} = \{(a,a) \in \mathbb{Z} \otimes \mathbb{Z}\}$$

$$\varphi^{-1}(3) = \{(a,b) \in \mathbb{Z} \otimes \mathbb{Z} : \varphi(a,b) = a - b = 3\}$$
$$= \{(a, a-3) \mid a \in \mathbb{Z}\}$$

٣-٢ حواصل الضرب الداخلية المباشرة Internal Direct Products

٣-٢-١ تعريف : لتكن H ، K زمرتين جزئيتين من زمرة G . يقال أن G حاصل الضرب الداخلى المباشر لـــ H ، K ونكتب $G = H \times K$ إذا تحقق الآتى :

(أ) $G = HK$ حيث $HK := \{hk \mid h \in H, k \in K\}$

(ب) $hk = kh$ لجميع $h \in H$ ، $k \in K$

(جـ) $H \cap K = \{e\}$ (e العنصر المحايد فى G)

ويعمم هذا التعريف كالآتى :

لتكن H_1 ، H_2 ، ... ، H_n زمراً جزئية من زمرة G . يقال إن G هى حاصل الضرب الداخلى المباشر لـــ H_1 ، H_2 ، ... ، H_n، ونكتب: $G = H_1 \times H_2 \times ... \times H_n$ إذا تحقق الآتى:

(أَ) $G = H_1 H_2 ... H_n := \{h_1 h_2 ... h_n \mid h_i \in H_i\}$

(بَ) $h_i h_j = h_j h_i \ \forall h_i \in H_i, h_j \in H_j, \ i \neq j$

(جـَ) $(H_1 H_2 ... H_i) \cap H_{i+1} = \{e\}, i = 1, 2, ..., n-1$

٣-٢-٢ نظرية : إذا كانت الزمرة G هى حاصل الضرب الداخلى المباشر للزمر الجزئية H_1 ، H_2 ، ... ، H_n فإن G تكون متشاكلة مع حاصل الضرب الخارجى المباشر للزمر الجزئية نفسها .

البرهان : ينتج من تعريف حاصل الضرب الداخلى المباشر أن كل عنصر فى G يمكن التعبير عنه بالشكل $h_1 h_2 .. h_n$ حيث $h_i \in H_i$. سنبرهن الآن على أن هذا التمثيل وحيد .

ليكن لدينا التمثيلان

$$g = h_1 h_2 \ldots h_n, g = k_1 k_2 \ldots k_n; h_i, k_i \in H_i, \quad i = 1, 2, \ldots, n.$$

أى أن :

$$h_1 h_2 \ldots h_n = k_1 k_2 \ldots k_n, h_i, k_i \in H_i, \quad i = 1, 2, \ldots, n \qquad (*)$$

$$\Rightarrow k_n h_n^{-1} = k_1^{-1} h_1 k_2^{-1} h_2 \ldots k_{n-1}^{-1} h_{n-1}$$ (الشرط (بَ) فى التعريف)

$$\Rightarrow k_n h_n^{-1} \in H_1 H_2 \ldots H_{n-1}, k_n h_n^{-1} \in H_n$$

$$\Rightarrow k_n h_n^{-1} \in H_1 H_2 \ldots H_{n-1} \cap H_n = \{e\}$$ (الشرط (جـَ) من التعريف)

$$\Rightarrow h_n = k_n$$

$$\Rightarrow h_1 h_2 \ldots h_{n-1} = k_1 k_2 \ldots k_{n-1}$$ (بحذف h_n ، k_n من *)

ونكرر ما سبق فنحصل على $h_{n-1} = k_{n-1}$. وبالتكرير نصل إلى أن $h_i = k_i$ لجميع $i = 1, \ldots, n$. أى أن التمثيل وحيد .

والآن نعرف :

$$\varphi : G \to H_1 \otimes H_2 \otimes \ldots \otimes H_n$$
$$(h_1 h_2 \ldots h_n) \mapsto (h_1, h_2, \ldots, h_n)$$

واضح أن φ راسم غامر (شامل)

ليكن $\varphi(h_1 h_2 \ldots h_n) = \varphi(k_1 k_2 \ldots k_n)$

أى أن

$$(h_1, h_2, \ldots, h_n) = (k_1, k_2, \ldots, k_n)$$
$$\Rightarrow h_1 = k_1, h_2 = k_2, \ldots, h_n = k_n$$

أى أن φ راسم واحد لواحد .

$$\forall (h_1 h_2 \ldots h_n), (k_1 k_2 \ldots k_n) \in G :$$

$$\varphi((h_1 h_2 \ldots h_n)(k_1 k_2 \ldots k_n)) = \varphi(h_1 h_2 \ldots h_n k_1 k_2 \ldots k_n)$$

$$= \quad \varphi(h_1 k_1 h_2 k_2 \ldots h_n k_n) = (h_1 k_1, h_2 k_2, \ldots, h_n k_n)$$

الشرط (ب)

(من تعريف حاصل الضرب الخارجى) $=(h_1,h_2,...,h_n)(k_1,k_2,...,k_n)$

هومورفيزم φ $= \varphi(h_1,h_2...h_n)\varphi(k_1k_2...k_n) \Rightarrow$

إذن φ أيزومورفيزم (تشاكل) . نهاية البرهان .

٣-٢-٣ ملحوظة : لاحظ الفرق بين حاصلى الضرب الداخلى والخارجى المباشرين . فى الداخلى يتم الضرب داخل الزمرة مستخدمين زمراً جزئية منها ، بينما حاصل الضرب الخارجى يمكن ان يتم لأية زمر ليس بينها أدنى علاقة ، وتتكون زمرة جديدة بعملية (= بضرب) جديدة (جديد)

٣-٢-٤ تعريف : إذا كان k قاسماً لـــ n فإننا نعرف

$$U_k(n) := \{x \in U(n) \mid x \equiv 1 \bmod(k)\}$$

٣-٢-٥ أمثلة :

مثال ١ : اختبر إذا ما كانت $H:=\{1,17\}$ ، $K:=\{1,13\}$ ، HK زمراً جزئية من $U(24)$

الحل : $(17)(17) = 289 \equiv 1(\bmod 24)$ إذن H زمرة جزئية من

$U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$

$(13)(13) = 169 \equiv 1(\bmod 24)$. إذن K زمرة جزئية من $U(24)$

$HK = \{1, 13, 17, 5\}$

$(13)(17) = 221 \equiv 5(\bmod 24)$

$(13)(5) = 65 \equiv 17(\bmod 24)$

$(17)(5) = 85 \equiv 13(\bmod 24)$

$(5)(5) = 25 \equiv 1(\bmod 24)$

إذن HK زمرة جزئية من $U(24)$

مثال ٢ : فى S_3 واضح أن $H: = \{e, (12)\}$ ، $K: = \{e, (13)\}$ حيث e العنصر المحايد فى S_3 زمرتان جزئيتان فى S_3 . هل HK زمرة جزئية من S_3 ؟

<u>الحـل</u> :

$HK = \{e, (12), (13), (12)(13)\} = \{ e, (12),(13), (132)\}$
$(13)(12) = (123) \notin HK$

إذن HK ليس زمرة جزئية من S_3 .

<u>مثالث ٣</u> : فى S_3 ليكن $H: = [(123)]$ ، $K: = [(12)]$. برهن على أن $HK = S_3$.

هل $H \otimes K \cong S_3$ ؟ لماذا ؟

<u>الحـل</u> : $H = \{e, (123), (132)\}$ ، $K = \{e, (12)\}$.

$HK = \{e, (12), (123), (132), (123)(12), (132)(12)\}$
$= \{e, (12), (123), (132), (13), (23)\} = S_3$

حسب النظرية (٣-١-٩) تكون $H \otimes K$ زمرة إبدالية ، بينما S_3 ليست زمرة إبدالية ، ولهذا $H \otimes K \ncong S_3$ وسبب هذا هو عدم تحقق الشرط (ب) فى التعريف (٣-٢-١) وبهذا لا يتم هذا التشاكل (انظر نظرية (٣-٢-٢)).

<u>مثال ٤</u> : إذا كانت $(\mathbb{R}^*_+,.)$ هى زمرة الأعداد الحقيقية الموجبة (أكبر من الصفر) مع عملية الضرب فبرهن على أن $(\mathbb{R} \setminus \{0\},.)$ هى حاصل الضرب المباشر لـ $(\mathbb{R}^*_+,.)$ مع الزمرة $\{1, -1\}$

<u>البرهان</u> : واضح أن : $\mathbb{R}^*_+.\{1,-1\} = \mathbb{R} \setminus \{0\}$

حيث إن $(\{1, -1\},.)$ ، $(\mathbb{R}^*_+,.)$ زمرتان جزئيتان من $(\mathbb{R} \setminus \{0\},.)$

كذلك فإن : $\mathbb{R}^*_+ \cap \{1,-1\} = \{1\}$

حيث 1 هو العنصر المحايد فى $(\mathbb{R} \setminus \{0\},.)$

وكذلك فإن الشرط (ب) فى التعريف (٣-٢-١) متتحقق لأن الضرب إبدالى فى $\mathbb{R}$ فينتج المطلوب

<u>٣-٢-٦ نظرية</u> : (بدون برهان)

ليكن s ، t ليس بينهما قواسم مشتركة . عندئذ فإن $U(st)$ هى حاصل الضرب الداخلى المباشر لـ $U_s(st)$ ، $U_t(st)$. كذلك فإن $U(st)$ تكون متشاكلة مع حاصل

الضرب الخارجى المباشر لـ $U(s)$ ، $U(t)$. علاوة على هذا فإن $U_s(st)$ تكون متشاكلة مع $U(t)$ ، $U_t(st)$ تكون متشاكلة مع $U(s)$. وباختصار فإن :

$$U(st) = U_s(st) \times U_t(st) \cong U(t) \otimes U(s)$$

٣-٢-٧ نتيجة : ليكن $m = n_1 n_2 ... n_k$ حيث $gcd(n_i, n_j) = 1, i \neq j$ (القاسم المشترك الأعظم). عندئذ فإن :

$$U(m) = U_{m/n_1}(m) \times U_{m/n_2}(m) \times ... \times U_{m/n_k}(m)$$
$$\cong U(n_1) \otimes U(n_2) \otimes ... \otimes U(n_k)$$

٣-٢-٨ مثال :

$$U(105) = U(15.7) = U_{15}(105) \times U_7(105)$$
$$= \{1, 16, 31, 46, 61, 76\} \times \{1, 8, 22, 29, 43, 64, 71, 92\}$$
$$\cong U(7) \otimes U(15),$$
$$U(105) = U(5.21) = U_5(105) \times U_{21}(105)$$
$$= \{1, 11, 16, 26, 31, 41, 46, 61, 71, 76, 86, 101\} \times \{1, 22, 43, 64\}$$
$$\cong U(21) \otimes U(5),$$
$$U(105) = U(3.5.7) = U_{35}(105) \times U_{21}(105) \times U_{15}(105)$$
$$= \{1, 71\} \times \{1, 22, 43, 64\} \times \{1, 16, 31, 46, 61, 76\}$$
$$\cong U(3) \otimes U(5) \otimes U(7)$$

٣-٢-٩ حسابات هامة لجاوس : النتائج التالية كان كارل جاوس أول من برهنها فى سنة ١٨٠١ :

$$U(2) \cong \{1\}, U(4) \cong \mathbb{Z}_2, U(2^n) \cong \mathbb{Z}_2 \otimes \mathbb{Z}_{2^{n-2}}, n \geq 3,$$

$U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}},$ $\quad p \in \mathbb{P} \setminus \{2\}$ (عدد فردى أولى)

٣-٢-١٠ أمثلة متنوعة :

مثال ١ :

$$U(105)=U(3.5.7) \underset{\text{٣-٢-٦}}{\cong} U(3)\otimes U(5)\otimes U(7)$$

$$\underset{\text{٣-٢-٩}}{\cong} \mathbb{Z}_2\otimes\mathbb{Z}_4\otimes\mathbb{Z}_6$$

$$U(720)=U(16.9.5) \underset{\text{٣-٢-٦}}{\cong} U(16)\otimes U(9)\otimes U(5)$$

$$\underset{\text{٣-٢-٩}}{\cong} \mathbb{Z}_2\otimes\mathbb{Z}_4\otimes\mathbb{Z}_6\otimes\mathbb{Z}_4$$

مثال٢ : اوجد عدد العناصر التى رتبتها 12 فى $U(720)$

الحـل : من مثال ١ $\quad U(720)\cong\mathbb{Z}_2\otimes\mathbb{Z}_4\otimes\mathbb{Z}_6\otimes\mathbb{Z}_4$

ومن النظرية (٣-١-٧) يكون العنصر المطلوب الذى بالشكل (a,b,c,d) يحقق :

(أ) $Ord(b)=4$ و $Ord(c)=6$ أو $Ord(c)=3$ (or)

أو (ب) $Ord(d)=4$ و $Ord(c)=6$ أو $Ord(c)=3$

فى الحالة (أ) : $c=\bar{1}$ أو $c=\bar{2}$ أو $c=\bar{4}$ أو $c=\bar{5}$ ،

$b=\bar{1}$ أو $b=\bar{3}$

بينما يمكن اختيار a ، d بدون قيود . $(a\in\mathbb{Z}_2 \quad ، \quad d\in\mathbb{Z}_4)$ وبهذا يكون لدينا فى الحالة (أ) 64 عنصراً لهم الرتبة 12 (لأن : $2.2.4.4=64$)

فى الحالة (ب) : لدينا من العناصر التى رتبتها 12 ولم ترد فى الحالة (أ) :

$2.2.4.2=32$ عنصراً

(هنا $Ord(b)=1$ أو $Ord(b)=2$ ، $a\in\mathbb{Z}_2$ بدون قيود ، أى أن

$b=\bar{4}=\bar{0}$ أو $b=\bar{2}$ ، $c=\bar{1}$ أو $c=\bar{2}$ أو $c=\bar{4}$ أو $c=\bar{5}$ ، $d=\bar{1}$ أو $d=\bar{3}$ ،

$a=\bar{1}$ أو $a=\bar{2}$)

ومن ثم يكون العدد الكلى للعناصر المطلوبة هو 96

مثال ٣ : اوجد اول رقمين من جهة اليمين فى العدد 49^{111}

الحــل : المطلوب هو إيجاد $49^{111} \pmod{100}$. لاحظ أن $49 \in U(100)$. والآن :

$$U(100) = U(4) \otimes U(25) \underset{\text{٩-٢-٣}}{\cong} \mathbb{Z}_2 \otimes \mathbb{Z}_{20}$$

وهذا يقتضى أن أى عنصر $x \in U(100)$ يحقق : $x^{20} \equiv 1 (\text{mod} 100)$

$$\Rightarrow 49^{111} = (49)^{100}(49)^{11} = (49^{20})^5 (49)^{11} = (1)^5 (49)^{11}$$

$$= 1.(7^2)^{11} = 7^{22} = 7^{20}.7^2 = 1.7^2 \equiv 49 (\text{mod} 100)$$

مثال ٤ : احسب $U_8(40)$ ، $U_5(40)$ ، $U(40)$. هل $U(40) = U_5(40) \times U_8(40)$ ؟ لماذا ؟

الحــل :

$U_8(40) = \{1, 9, 17, 33\}$

$U_5(40) = \{1, 11, 21, 31\}$

$$U_8(40) \times U_5(40) = \{1,11,21,31,9,19,29,39,17,27,37,7,33,3,13,23\}$$
$$= U(40)$$

من النظرية (٣-٢-٦) يجب أن يكون : $U_8(40) \times U_5(40) = U(40)$

مثال ٥ : احسب $U(20)$ ، $U_4(20)$ ، $U_{10}(20)$. هل $U(20)$ هى حاصل الضرب الداخلى المباشر لــ $U_4(20)$ ، $U_{10}(20)$ ؟ هل يتناقض هذا مع النظرية (٣-٢-٦) ؟

الحــل :

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$U_4(20) = \{1, 9, 13, 17\}$

$U_{10}(20) = \{1, 11\}$

$$U_4(20) \times U_{10}(20) = \{1,11,9,19,13,3,17,7\} = U(20)$$

نعم $U(20)$ هى حاصل الضرب الداخلى المباشر لــ $U_4(20)$ ، $U_{10}(20)$. ولايتناقض هذا مع النظرية (٣-٢-٦) ، فالنظرية (٣-٢-٦) تعطى شرطاً كافياً لأن يكون $U(st)$

هو حاصل الضرب الداخلى المباشر لـــ$U_s(st)$ ، $U_t(st)$ وهو ألا يكون s ، t لهما قواسم مشتركة (ماعدا الواحد). وهذا الشرط ليس ضرورياً ولم يتحقق فى المثال المعطى .

مثال ٦ : برهن على أن D_4 (الزمرة الزوجية الثنائية . انظر مثال ٤٨ من أمثلة متنوعة على الباب الأول) لايمكن التعبير عنها كحاصل ضرب داخلى مباشر من زمرتين جزئيتين فعليتين

البرهان : لنفترض أنه أمكن كتابة D_4 كحاصل ضرب داخلى مباشر لزمرتين جزئيتين فعليتين من D_4 هما H ، K حيث $\alpha:=\begin{pmatrix}1&2&3&\dots&n\\2&3&4&\dots&1\end{pmatrix}\in H$ ، $\beta:=\begin{pmatrix}1&2&3&\dots&n\\1&n&n\text{-}1&\dots&2\end{pmatrix}\in K$

من النظرية (٣-٢-٢) ينتج أن D أيزومورفية (متشاكلة) مع حاصل الضرب الخارجى لـــ H ، K أى أن:

$$D_4 \cong H \otimes K$$

جميع الزمر الجزئية الفعلية من D_4 تكون إبدالية ، بينما أن D_4 ليست إبدالية ، لأن :

$$\beta\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8\\1&8&7&6&5&4&3&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&5&6&7&8&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&6&5&4&3&2&1\end{pmatrix}=(1\ \ 8)(2\ \ 7)(3\ \ 6)(4\ \ 5)$$

بينما

$$\alpha\beta=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&5&6&7&8&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\1&8&7&6&5&4&3&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&1&8&7&6&5&4&3\end{pmatrix}=(1\ \ 2)(3\ \ 8)(4\ \ 7)(5\ \ 6)$$

أى أن

$$\alpha\beta \neq \beta\alpha$$

وهنا يتناقض مع أن D_4 إبدالية إذا كان وفقط إذا كان H ، K إبداليتين (انظر مثال ١٢ فى (٣-١-١٣))

مثال ٧ : برهن على أن S_3 ليست حاصل ضرب داخلى مباشر للزمرتين الجزئيتين :
$H := \{e, (1\,2\,3), (1\;3\;2)\}$ ، $K := \{e, (2\;\;3)\}$ (e عنصر S_3 المحايد)

البرهان : الحل مشابه لحل المثال ٦ السابق مباشرة : H ، K زمرتان جزئيتان فعليتان إبداليتان من S_3 بينما S_3 – كما تعلم – ليست إبدالية . فلو كانت S_3 حاصل ضرب داخلى مباشر لـ H ، K كانت S أيضاً متشاكلة مع حاصل الضرب الخارجى لهما. وكانت بالتالى إبدالية (مثال١٢ فى (٣-١-١٣)) هذا يتناقض مع كونها ليست إبدالية .

مثال ٨ : فى S_3 لتكن $H := \{e, (2\;\;3)\}$ ، $K := \{e, (1\;\;3)\}$. أوجد HK ، $[HK]$ (تقاطع جميع الزمر الجزئية التى تحتوى على HK ، أى أصغر زمرة جزئية تحتوى على HK . انظر (١-١١-٢))
(e عنصر S_3 المحايد)

الحل :

$$HK = \{e, (2\,3)\}\{e, (1\,3)\} = \{e, (1\,3), (2\,3), (2\,3)(1\,3)\}$$
$$= \{e, (1\,3), (2\,3), (1\,2\,3)\}$$

أى زمرة جزئية تحتوى على HK تحتوى على جميع معكوسات عناصر HK ومن ثم فهى تحتوى على $(1\,3\,2)$ الذى هو معكوس $(1\,2\,3)$. كذلك هى تحتوى على جميع "حواصل ضرب" عناصرها ، فهى تحتوى على

$(1\,3)(1\,2\,3)$. أى أنها تحتوى كذلك على $(1\,3)(1\,2\,3) = (1\,2)$

ومن ثم فإن : $[HK] = S_3$

مثال ٩ : اعتبر الزمرتين $H := [2]$ ، $K := [6]$ من $\mathbb{Z}_{12}$. احسب HK ، $[HK]$

الحل : لاحظ أن العملية فى $\mathbb{Z}_{12}$ هى الجمع مقياس 12 ، وبهذا يكون :

$$HK = \{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\} + \{\bar{0},\bar{6}\} = \{\bar{0},\bar{2},,\bar{4},\bar{6},\bar{8},\overline{10}\} = [\bar{2}]$$

كذلك فإن $[HK]$ وهى أصغر زمرة جزئية تحتوى على HK ، هى نفسها $[\bar{2}]$

مثال ١٠ : ليكن $n = rs$ حيث r ، s عددان صحيحان ليس لهما قواسم مشتركة أى أن $gcd(r,s) = 1$. برهن على أن $\mathbb{Z}_n$ هى حاصل الضرب الداخلى المباشر لزمرتيها الجزئيتين الدائريتين $[r]$ ، $[s]$.

البرهان : الحساب مقياس n .

لأن $gcd(r,s)=1$ فإن : $[r]+[s]=[1]$

$$(1) \qquad \Rightarrow [r]+[s]=\mathbb{Z}_n$$

ليكن $0 \neq z \in [r] \cap [s]$. هذا يقتضى أنه يوجد $x, y \in \mathbb{Z}_n$ أى أن $0 < x,y < n$ بحيث

إن : $z=xr=ys<n$. هذا يقتضى أن $rsxy<n^2$ أى أن $xy<n$ (لأن $rs=n$) (*)

من حيث إن $xr=ys$، $gcd(r,s)=1$ ينتج أن r قاسم لـــ y . كذلك فإنه ينتج أن s قاسم لـــ x

أى أن rs قاسم لـــ xy أى أن n قاسم لـــ xy . وهذا تناقض مع(*). إذن $[r] \cap [s]=\{0\}$ (2)

والجمع إبدالى فى $\mathbb{Z}_n$ (3) . من (1) ، (2) ، (3) ينتج المطلوب مباشرة .

مثال ١١: اعتبر الزمرتين الجزئيتين $H:=\{e,(13)\}$ ، $K:=\{e,(24)\}$ من الزمرة D_4 (زمرة تناظرات المربع (انظر مثالى ٤٥ ، ٤٨ من أمثلة متنوعة على الباب الأول).

اوجد HK ، $[HK]$

الحـــل :

$$HK=\{e,(13)\}\{e,(24)\}=\{e,(13),(24),(13)(24)\}$$

واضح أن HK زمرة جزئية من D_4 ، وبالتالى فإن اصغر زمرة جزئية من D_4 تحتوى عليها (على HK) هى HK نفسها ، أى أن $[HK]=HK$

مثال ١٢ : اوجد اكبر رتبة للعناصر فى $U(900)$

الحـــل :

$$U(900)=U(4.\,9.\,25)=U(4.\,3^2\,.\,5^2)$$

$$\cong \quad \mathbb{Z}_2 \otimes \mathbb{Z}_{3^2-3} \otimes \mathbb{Z}_{5^2-5}=\mathbb{Z}_2 \otimes \mathbb{Z}_6 \otimes \mathbb{Z}_{20}$$

٣-٢-٦

٣-٢-٩

وتكون أكبر رتبة للعناصر فى $U(900)$ هى $\ell cm\{2,6,20\}$

$$=60$$

(انظر النظرية (٣-١-٧))

مثال ١٣ : لتكن H ، K زمرتين جزئيتين من الزمرة G . إذا كانت $G=HK$ ، $g=hk$ حيث $h\in H$ ، $k\in K$ ، فهل توجد أية علاقة بين رتبة (g) ، رتبة (h) ، رتبة (k) ؟

وإذا كانت $G=H\times K$، أى حاصل الضرب الداخلى المباشر لـــ H ، K ، فهل توجد علاقة ؟

الحـــل : فى الحالة الأولى لاتوجد أية علاقة . فى الحالة الثانية التى فيها $G=H\times K$ فإننا نعلم من النظرية (٣-١-٧) أن

$$Ord(g)=\ell cm\{Ord(h),Ord(k)\}$$

مثال ١٤ : ليكن p ، q عددين أوليين فرديين ، m ، n عددين صحيحين موجبين .

وضح لماذا $U(p^m)\otimes U(q^n)$ ليست زمرة دائرية .

الحـــل :

$$U(p^m)\cong\mathbb{Z}_{p^m-p^{m-1}}=\mathbb{Z}_{2r} \qquad (\text{لأن } p \text{ فردى أولى})$$

$$U(q^n)\cong\mathbb{Z}_{q^n-q^{n-1}}=\mathbb{Z}_{2s} \qquad (q \text{ عدد فردى أولى})$$

من النظرية (٣-١-٩) ستكون $U(p^m)\otimes U(q^n)$ دائرية إذا كان $Ord\,(U(p^m))$ ، $Ord\;U(q^n)$ ليس بينهما قواسم مشتركة (عدا ± 1) وهذا غير متحقق لأن 2 قاسم مشترك لكلتا الرتبتين.

مثال ١٥ : برهن على أن $U(144)\cong U(140)$

البرهان :

$$U(144)=U(2^4.3^2)$$

$$\underset{\text{٣-٢-٦}}{\cong}\; U(2^4)\otimes U(3^2) \qquad (\text{لأن } gcd(2,3)=1)$$

$$\underset{\text{٣-٢-٩}}{\cong}\; \mathbb{Z}_2\otimes\mathbb{Z}_{2^{4-2}}\otimes\mathbb{Z}_{3^2-3}=\mathbb{Z}_2\otimes\mathbb{Z}_4\otimes\mathbb{Z}_6 \qquad (1)$$

$$U(140)=U(4.5.7)\;\underset{\text{٣-٢-٦}}{\cong}\; U(4)\otimes U(5)\otimes U(7)$$

(لأن $gcd(5, 7) = 1$ ، $gcd(4, 7) = 1$ ، $gcd(4, 5) = 1$)

$$\cong \quad \mathbb{Z}_2 \otimes \mathbb{Z}_{5-5^0} \oplus \mathbb{Z}_{7-7^0} = \mathbb{Z}_2 \otimes \mathbb{Z}_4 \otimes \mathbb{Z}_6 \qquad (2)$$

٣-٢-٩

من (1) ، (2) ينتج المطلوب مباشرة .

مثال ١٦ : فى $\mathbb{Z}$ ليكن $H := [4]$ ، $K := [10]$. عبر عن HK على الشكل $[g]$.

عمم هذه الحالة حيث $H = [a]$ ، $K = [b]$

الحل : (العملية هنا الجمع) $[4] + [10] = [gcd\{4, 10\}]$

$$= [2]$$

$$[a] + [b] = [gcd\{a, b\}]$$

مثال ١٧ : فى $\mathbb{Z}$ ليكن $H := [5]$ ، $K := [7]$. برهن على أن $\mathbb{Z} = HK$. هل $\mathbb{Z} = H \times K$ أى حاصل الضرب الداخلى المباشر لـــ H ، K ؟

الحـــل : (العملية هى الجمع)

$$[5] + [7] = [gcd\{5, 7\}] = [1]$$

$$= \mathbb{Z}$$

$$0 \neq 35 \in [5] \cap [7] \Rightarrow \mathbb{Z} \neq H \times K$$

مثال ١٨ : لتكن

$$G := \left\{ \begin{pmatrix} \bar{1} & a & b \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \middle| a,b,c \in \mathbb{Z}_3 \right\} \text{ ،} \quad H := \left\{ \begin{pmatrix} \bar{1} & a & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \middle| a \in \mathbb{Z}_3 \right\} \text{ ،}$$

$$K := \left\{ \begin{pmatrix} \bar{1} & \bar{0} & b \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \middle| b \in \mathbb{Z}_3 \right\} \text{ ،} \quad L := \left\{ \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \middle| c \in \mathbb{Z}_3 \right\}$$

برهن على أن $G = HKL$ ، هل $G = H \times K \times L$?

الحـــل : واضح أن $HKL \subset G$. نبرهن على أن $G \subset HKL$ كالآتى :

ليكن $\begin{pmatrix} \bar{1} & a & b \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in G$ ، $\begin{pmatrix} \bar{1} & x & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in H$ ، $\begin{pmatrix} \bar{1} & \bar{0} & y \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in K$ ،

$\begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & z \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in L$ حيث $a,b,c,x,y,z \in \mathbb{Z}_3$

والآن

$$\begin{pmatrix} \bar{1} & x & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{1} & \bar{0} & y \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & z \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & a & b \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} \bar{1} & x & xz+y \\ \bar{0} & \bar{1} & z \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & a & b \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \Rightarrow x = a, z = c,$$

$$y = b - ac,$$

$$x, y, z \in \mathbb{Z}_3$$

أى أن $G \subset HKL$

أى أن $G = HKL$

والآن
$$\begin{pmatrix} \bar{1} & a & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & a & ac \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

بينما
$$\begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{1} & a & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & a & \bar{0} \\ \bar{0} & \bar{1} & c \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

إذن الشرط (ب) فى (٣-٢-١) ليس متحققاً ، وبهذا $G \neq H \times K \times L$

ملحوظة : لاحظ أن

$\det(g)=\det(h)=\det(k)=\det(\ell)=1\neq 0$ لجميع $g\in G$ ، $h\in H$ ، $k\in K$ ، $\ell\in L$ ، والعملية هى ضرب المصفوفات

<u>مثال ١٩</u> : برهن على أنه لكل $n>2$:

$$U(n)^2 := \{x^2 \mid x\in U(n)\}$$

زمرة جزئية فعلية (مضبوطة) من $U(n)$.

<u>البرهان</u> :

(i) $1\in U(n) \Rightarrow 1=1^2\in U(n)^2$

(ii) $x^2, y^2\in U(n)^2 \Rightarrow x,y\in U(n) \Rightarrow xy\in U(n) \Rightarrow x^2y^2=(xy)^2\in U(n)^2$

(iii) $x^2\in U(n)^2 \Rightarrow x\in U(n) \Rightarrow x^{-1}\in U(n) \Rightarrow (x^2)^{-1}=(x^{-1})^2\in U(n)^2$

$\Rightarrow U(n)^2 \hookrightarrow U(n)$ ($U(n)^2$ زمرة جزئية من $U(n)$)

لاثبات أن $U(n)^2$ زمرة جزئية <u>فعلية</u> من $U(n)$. خذ $x<n$ عدداً طبيعياً ، $gcd(x, n)=1$ ، $\sqrt{x}\notin\mathbb{N}$. ينتج أن $x\in U(n)$ ، $x\notin U(n)^2$. إذا كانت n فردية خذ $x=2$.

<u>مثال ٢٠</u> : عبر عن $Aut(\mathbb{Z}_2\otimes\mathbb{Z}_3\otimes\mathbb{Z}_5)$ كحاصل ضرب خارجى مباشر لزمر على الشكل $\mathbb{Z}_n$

<u>الحـل</u> : من النتيجة (٣-١-١١) نعلم أن

$$Aut(\mathbb{Z}_2\otimes\mathbb{Z}_3\otimes\mathbb{Z}_5)\cong Aut(\mathbb{Z}_{2\times3\times5})$$

كذلك نعلم أن $Aut(\mathbb{Z}_n)\cong U(n)$ (تمرين ٨٥ من تمارين عامة على الباب الأول) ، ومن ثم فإن :

$Aut(\mathbb{Z}_2\otimes\mathbb{Z}_3\otimes\mathbb{Z}_5)\cong U(2\times3\times5)\cong U(2)\otimes U(3)\otimes U(5)$ (من ٣-٢-٦)

$\cong \{1\}\otimes\mathbb{Z}_{3-1}\otimes\mathbb{Z}_{5-1}$ (من ٣-٢-٩)

$\cong \mathbb{Z}_2\otimes\mathbb{Z}_4$

مثال ٢١: بدون إجراء حسابات فى $Aut(\mathbb{Z}_{50})$ برهن على أن $Aut(\mathbb{Z}_{50})$ دائرية .

البرهان :
$$Aut(\mathbb{Z}_{50}) \cong U(50) \cong U(2) \otimes U(25) = U(2) \times U(5^2)$$
$$\cong \{1\} \otimes \mathbb{Z}_{5^2-5} \cong \mathbb{Z}_{20}$$

وهى دائرية .

مثال ٢٢ : بدون إجراء حسابات فى $U(27)$ اوجد عدد الزمر الجزئية الفعلية فى $U(27)$

الحــل :
$$U(27) = U(3^3) \cong \mathbb{Z}_{3^3-3^2} = \mathbb{Z}_{18}$$

ومن الإستنتاج (١-١١-١٢) يكون لدينا أربع زمر جزئية فعلية من $U\ (27)$ رتبها 2 ، 3 ، 6 ، 9 (قواسم 18)

مثال ٢٣ : برهن على أنه توجد زمرة U (U-group) تحتوى على زمرة جزئية تكون متشاكلة (أيزومورفية) مع $\mathbb{Z}_3 \otimes \mathbb{Z}_3$

البرهان :
$$U(63) = U(3^2.7) \cong U(3^2) \otimes U(7)$$
$$\cong \mathbb{Z}_{3^2-3} \otimes \mathbb{Z}_6 \cong (\mathbb{Z}_2 \otimes \mathbb{Z}_3) \otimes (\mathbb{Z}_3 \otimes \mathbb{Z}_2)$$
$$= \mathbb{Z}_2 \otimes (\mathbb{Z}_3 \otimes \mathbb{Z}_3) \otimes \mathbb{Z}_2$$

مثال ٢٤ : لتكن $G := \{3^a 6^b 10^c \mid a,b,c \in \mathbb{Z}\}$ والعملية هى الضرب العادى ، ولتكن $H := \{3^a 6^b 12^c \mid a,b,c \in \mathbb{Z}\}$ والعملية هى الضرب العادى كذلك . برهن على أن : $G = [3] \times [6] \times [10]$ بينما $H \neq [3] \times [6] \times [12]$

البرهان : واضح أن $[3] = \{3^x \mid x \in \mathbb{Z}\}$ لأن [3] ، [6] ، [10] يجب أن تكون زمراً جزئية من G حتى يتحقق $G = [3] \times [6] \times [10]$ وواضح بالفعل أن $G = [3][6][10]$.
كذلك ضرب الأعداد إبدالى ، وكذلك

فإن : $[3] \cap [6] = \{1\}$ ، $[3][6] \cap [10] = \{1\}$ وهذا يكفى حتى يتحقق الشرط (جـ) .
إذن G هى حاصل الضرب الداخلى لــ [3] ، [6] ، [10] .

بينما $3^{-1}.6^{2}=12\in[12]$ ، أى أن $[3][6]\cap[12]\neq\{1\}$ أى أن الشرط (جـ) فى التعريف (٣-٢-١) غير متحقق . نهاية البرهان .

مثال ٢٥ : هل $U(30)/U_5(30)$ تتشاكل مع $\mathbb{Z}_4$ أم مع $\mathbb{Z}_2\otimes\mathbb{Z}_2$ ؟

الحـــل :

$$U(30)=\{1,7,11,13,17,19,23,29\}$$

$$U_5(30)=\{1,11\}=H$$

الضرب مقياس 30 : $U(30)/U_5(30)=\{1H,7H,11H,13H,17H,19H,23H,29H\}$

لاحظ أن : $1H,\ 11\,H=H$

$$17H=17\{1,11\}=\{17,187\}=\{17,7\}=7\{11,1\}=7\,H$$

$$23\,H=23\{1,11\}=\{23,253\}=\{23,13\}=\{143,13\}=13\{11,1\}=13\,H,$$

$$29\,H=29\{1,11\}=\{29,319\}=\{29,19\}=\{209,19\}=19\,\{11,1\}=19\,H$$

$$\Rightarrow U(30)/U_5(30)=\{H,7H,13H,19H\}$$

وهى دائرية يصلح كمولد لها $7H$ (كما يصلح $13\,H$ مولداً لها ، أما $19\,H$ فلا يصلح لأن رتبة $19\,H$ هى 2)

وبالتالى فهى تتشاكل مع $\mathbb{Z}_4$ وليس مع $\mathbb{Z}_2\otimes\mathbb{Z}_2$

مثال ٢٦ : ما رتبة الزمرة $\mathbb{Z}_{10}\otimes U(10)/[(2,9)]$ ؟

$$U(10)=\{1,3,7,9\}$$

$$[(2,9)]=\{(2,9),(4,1),(6,9),(8,1),(0,9),(2,1),(4,9),(6,1),(8,9),(0,1)\}$$

$$Ord([(2,9)])=10\ ,\ Ord(\mathbb{Z}_{10}\otimes U(10))=10\times4=40$$

$$Ord(\mathbb{Z}_{10}\otimes U(10)/[(2,9)])=\frac{40}{10}=4$$

مثال ٢٧ : إذا كانت $G = HK$ حيث G زمرة ، H ، K زمرتان جزئيتان طبيعيتان فى G ، $H \cap K = \{e\}$ ، حيث e العنصر المحايد فى G . برهن على أن G هى حاصل الضرب الداخلى المباشر لـ H ، K .

البرهان : من مثال٤٠ فى أمثلة متنوعة على الباب الأول ينتج أن $hk = kh$ لجميع $h \in H$ ، $k \in K$. وينتج المطلوب مباشرة .

تمارين

(١) اوجد رتبة كل عنصر فى $\mathbb{Z}_3 \otimes \mathbb{Z}_6$

(٢) هل $\mathbb{Z}_3 \otimes \mathbb{Z}_9$ متشاكلة مع $\mathbb{Z}_{27}$ ؟ لماذا ؟

(٣) هل $\mathbb{Z}_3 \otimes \mathbb{Z}_5$ متشاكلة مع $\mathbb{Z}_{15}$ ؟ لماذا ؟

(٤) الزمرة الثنائية (المزدوجة) D_n لها الرتبة $2n$ ، ولها زمرتان جزئيتان واحدة تتكون من n دوراناً، والأخرى (الانعكاس) من الرتبة 2 . وضح لماذا لاتعتبر D_n متشاكلة مع حاصل الضرب الخارجى المباشر لهاتين الزمرتين الجزئيتين .

(٥)برهن على أن زمرة الأعداد المركبة مع عملية الجمع تكون متشاكلة مع الزمرة$\mathbb{R}\otimes\mathbb{R}$

(٦) اوجد رتبة أى عنصر لايساوى الوحدة فى $\mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$

(٧) اوجد جميع الزمر الجزئية من الرتبة الثالثة فى $\mathbb{Z}_9 \otimes \mathbb{Z}_3$

(٨) لتكن M زمرة المصفوفات من النوع 2×2 ، ومداخلها (عناصرها) أعداد حقيقية مع عملية جمع المصفوفات ، ولتكن $N=\mathbb{R}\otimes\mathbb{R}\otimes\mathbb{R}\otimes\mathbb{R}$ مع عملية جمع المركبات.(componentwise addition)

برهن على أن M ، N متشاكلتان (أيزومورفيتان). ما الذى يقابل العبارة السابقة إذا كانت المصفوفات من النوع $n\times n$ ؟

(٩) برهن على أن $D_3 \otimes D_4 \not\cong D_{24}$

(١٠) اوجد عدد الزمر الجزئية الدائرية من الرتبة 15 فى $\mathbb{Z}_{90} \otimes \mathbb{Z}_{36}$

(١١) أكمل الجمل الآتية :

(أ) الزمرة الجزئية الدائرية من $\mathbb{Z}_{24}$ التى تتولد من العنصر 18 لها الرتبة ---

(ب) $\mathbb{Z}_3 \otimes \mathbb{Z}_4$ من الرتبة ----

(جـ) العنصر (2 , 4) من الزمرة $\mathbb{Z}_{12} \otimes \mathbb{Z}_8$ له الرتبة ------

(د) زمرة كلاين الرباعية متشاكلة مع $\mathbb{Z}_{_} \otimes \mathbb{Z}_{_}$.

(هـ) $\mathbb{Z}_2 \otimes \mathbb{Z} \otimes \mathbb{Z}_4$ لها عدد – من العناصر التى رتبتها منتهية

(١٢) مهملاً ترتيب العوامل اكتب حاصل ضرب خارجى مباشر لاثنين أو لأكثر من الزمر التى على الشكل $\mathbb{Z}_n$ بحيث يكون الناتج متشاكلاً مع $\mathbb{Z}_{60}$ بكل الطرائق الممكنة .

(١٣) اوجد جميع الزمر الجزئية الفعلية فى $\mathbb{Z}_2 \otimes \mathbb{Z}_2$

(١٤) اوجد جميع الزمر الجزئية من $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_4$ التى تكون متشاكلة مع زمرة كلاين الرباعية.

(١٥) اضرب مثالاً لبيان أن ليست كل زمرة إبدالية هى حاصل ضرب داخلى مباشر لزمرتين جزئيتين فعليتين

(١٦)تذكر أنه إذا كانت K، H زمرتين جزئيتين من زمرة G فإن $HK=\{hk \mid h\in H, k\in K\}$. فى $U(24)$ عين المجموعتين $U_4(24)$ ، $U_6(24)$. هل $U(24) = U_4(24)\, U_6(24)$ ؟ هل حاصل الضرب داخلى ؟ لماذا ؟

(١٧) عبر عن $U(165)$ كحاصل ضرب خارجى مباشر لزمر U بثلاث طرائق مختلفة .

(١٨) عبر عن $U(165)$ كحاصل ضرب داخلى مباشر لزمر جزئية فعلية بثلاث طرائق مختلفة .

(١٩) عبر عن $U(165)$ كحاصل ضرب خارجى مباشر لزمر دائرية (عمليات جمع !) على الشكل $\mathbb{Z}_n$.

(٢٠) بدون إجراء حسابات فى $U(81)$ قرر عدد الزمر الجزئية فى $U(81)$

(٢١) اوجد عدد العناصر في $Aut(\mathbb{Z}_{720})$ التي رتبتها 6 بدون إجراء حسابات في $Aut(\mathbb{Z}_{720})$

(٢٢) بدون اجراء حسابات في $Aut(\mathbb{Z}_{20})$ اوجد عدد العناصر التي رتبتها 2 والتي رتبتها 4 .

(٢٣) برهن على أن : $U(55) \cong U(75)$

(٢٤) برهن على أنه توجد زمرة-U تحتوى على زمرة جزئية متشاكلة مع $\mathbb{Z}_{14}$

(٢٥) برهن على أنه لاتوجد زمرة $-U$ تحتوى على زمرة جزئية متشاكلة مع $\mathbb{Z}_4 \otimes \mathbb{Z}_4$

(٢٦) برهن على أنه لايمكن كتابة الزمرة $\mathbb{Z}_4$ كحاصل ضرب خارجي مباشر لزمرتين جزئيتين منها رتبة كل منهما 2 (العملية جمع)

(٢٧) برهن على أنه لايمكن كتابة الزمرة $\mathbb{Z}_8$ كحاصل ضرب خارجي مباشر لزمرتين جزئيتين غير تافهتين منها .

(٢٨) قرر إذا ما كانت العبارات الآتية صحيحة أم خاطئة :

(أ) لأى زمرتين G_2 ، G_1 يكون $G_1 \otimes G_2 \cong G_2 \otimes G_1$

(ب) أى زمرة ذات رتبة هى عدد أولى لايمكن أن تكون حاصل ضرب داخلى مباشر لزمرتين جزئيتين فعليتين منها .

(جـ) $\mathbb{Z}_2 \otimes \mathbb{Z}_4 \cong \mathbb{Z}_8$

(د) $\mathbb{Z}_4 \otimes \mathbb{Z}_4 \cong S_8$

(هـ) $\mathbb{Z}_3 \otimes \mathbb{Z}_8 \cong S_4$

(و) $Ord(\mathbb{Z}_{12} \otimes \mathbb{Z}_{15}) = 60$

(٢٩) ما أصغر زمرة غير إبدالية رتبتها عدد فردى ؟

(٣٠) ما أصغر عدد غير أولى لايساوى الواحد بحيث توجد زمرة وحيدة يكون رتبتها ؟

(٣١) أكمل :

(أ) الزمرة العاملة $(\mathbb{Z}_4 \otimes \mathbb{Z}_{12}) / ([2]\times[2])$ رتبتها ----

(ب) الزمرة العاملة $(\mathbb{Z}_4 \otimes \mathbb{Z}_{12}) / [(2,2)]$ رتبتها ----

(٣٢) اوجد عدد المجموعات المشاركة للزمر الجزئية الآتية.:

(أ) $[\overline{18}]$ فى $\mathbb{Z}_{36}$

(ب) $[\bar{1}]\otimes[\bar{0}]\otimes[\bar{0}]$ فى $\mathbb{Z}_3 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_4$

(جـ) $[\bar{0}]\otimes[\bar{1}]\otimes[\bar{2}]$ فى $\mathbb{Z}_3 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_4$

الباب 4

النظرية الأساسية للزمر الإبدالية المنتهية

Fundamental Theorem of Finite Abelian Groups

٤-١ النظرية الأساسية

٤-١-١ نظرية : كل زمرة إبدالية منتهية تكون حاصل ضرب (خارجى) مباشر لزمر دائرية رتبتها هى قوة (أسpower) لعدد أولى. وعلاوة على هذا فإن هذا التحليل (factorization) وحيد فيما عدا ترتيب العوامل .

ولأن أى زمرة دائرية منتهية G من الرتبة n تكون متشاكلة (أيزومورفية) مع $\mathbb{Z}_n$ (١-١١-٨)فإن النظرية تعنى أن كل زمرة إبدالية منتهية تكون متشاكلة مع زمرة لها الشكل :

$$\mathbb{Z}_{p_1^{n_1}} \otimes \mathbb{Z}_{p_2^{n_2}} \otimes \ldots \otimes \mathbb{Z}_{p_m^{n_m}} \qquad (*)$$

حيث الـــ p_i's أعداد أولية ليست بالضرورة مختلفة ، $p_1^{n_1}$ ، $p_2^{n_2}$ ، ... ، $p_m^{n_m}$ تتحدد وحدانيتها (uniquely determined) بـــ G .

٤-١-٢ تعريف : تسمى كتابة أى زمرة بالشكل (*) السابق **تحديد فصل التشاكل لـــ G**
(Determining the isomorphism class of G)

٤-١-٣ تمهيدية : لتكن G زمرة إبدالية منتهية من الرتبة mn حيث m ، n ليس لهما قواسم مشتركة . إذا كانت $H := \{x \in G \mid x^m = e\}$ وكانت $K := \{x \in G \mid x^n = e\}$ ، حيث e عنصر G المحايد فإن $G=H\times K$ (حاصل الضرب الداخلى المباشر لـــ H ، K)

البرهان : لأن G إبدالية فإننا بحاجة فقط إلى إثبات أن $G = HK$ ، وأن $H \cap K = \{e\}$.

من حيث إن $gcd(m, n) = 1$ فإنه يوجد عددان صحيحان s ، t بحيث إن $1 = sm + tn$.

والآن لأى $x \in G$ لدينا : $x = x^1 = x^{sm+tn} = x^{sm}x^{tn}$ ولكن : $(x^{sm})^n = (x^s)^{mn} = e$ من النتيجة (١-١١-٩) (٢) وبالتالى فإن $x^{sm} \in K$ وكذلك فإن $(x^{tn})^m = (x^t)^{mn} = e$ ، أى أن $x^{tn} \in H$. وهكذا فإن $G = HK$.

والآن ليكن $x \in H \cap K$. عندئذ فإن : $x^m = e = x^n$ فمن النتيجة (١-١١-٩) (١) ينتج أن رتبة (x) تقسم كلاً من m ، n . ومن حيث إن $gcd(m, n) = 1$ فإن $Ord(x) = 1$ ، وبالتالى فإن $x = e$. نهاية البرهان .

٤—١—٤ نتيجة : لتكن G زمرة إبدالية ولتكن $Ord(G)=p_1^{n_1}p_2^{n_2}...p_m^{n_m}$ حيث الـ p_i's كلها أعداد أولية مختلفة. ولتكن $G(p_i):=\{x\in G \mid x^{p_i^{n_i}}=e\}$ عندئذ فإنه من التمهيدية (٤-١-٣) وبالاستقراء الرياضى يكون

$$G=G(p_1)\times G(p_2)\times...\times G(p_n)$$

ومن ثم فإنه يكفى أن نعتبر الزمر ذات الرتبة من قوى عدد أولى .

٤-١-٥ تمهيدية : لتكن G زمرة إبدالية رتبتها قوة لعدد أولى وعنصرها المحايد e ، وليكن a عنصراً فى G له أكبر رتبة فيها . عندئذ فإنه يمكن كتابة G على الشكل : $G=[a]\times K$ (أى حاصل الضرب الداخلى (المباشر) لـ $[a]$ ، K)

البرهان : لتكن $Ord(G)=p^n$ ، وسنجرى الاستقراء الرياضى على n . إذا كانت $n=1$ فإن $G=[a]\times[e]$. (تذكر أنه إذا كانت رتبة زمرة ما عدداً أولياً كانت الزمرة دائرية . نظرية (١-١١-٧) (٢).) لنفترض أن المقولة صحيحة لجميع الزمر الإبدالية التى من الرتبة p^k حيث $k<n$.

والآن خذ العنصر a الذى له أكبر رتبة p^m من بين جميع عناصر G . (تذكر أن رتبة أى عنصر تقسم رتبة الزمرة المنتهية التى ينتمى إليها.) عندئذ فإن $x^{p^m}=e$ لجميع $x\in G$. وليكن $G\neq[a]$ ، وإلا يكون البرهان قد اكتمل . اختر العنصر b من بين عناصر G الذى يكون له أصغر رتبة بحيث إن $b\notin[a]$. سنبرهن على أن $[a]\cap[b]=\{e\}$: وذلك بالبرهنة على أن : $Ord(b)=p$. لأن $Ord(b^p)=\dfrac{Ord(b)}{p}$ نستنتج أن $b^p\in[a]$ بالطريقة التى اخترنا بها b. ليكن $b^p=a^i$. لاحظ أن: $e=b^{p^m}=(b^p)^{p^{m-1}}=(a^i)^{p^{m-1}}$ ، وهكذا فإن : $Ord(a^i)\leq p^{m-1}$. وهكذا فإن a^i ليس مولداً لـ $[a]$ ، ومن ثم فإنه من الاستنتاج (١-١١-١١) يكون $gcd(p^m,i)\neq 1$. وهذا يبرهن على أن p يقسم i ، وبالتالى فإنه يمكننا

أن نكتب : $i = pj$. وعندئذ فإن : $b^p = a^i = a^{pj}$. والآن اعتبر العنصر $c = a^{-j}b$. c لايقع فى $[a]$ وإلا وقعت b كذلك فى $[a]$. كذلك فإن:

$c^p = a^{-jp}b^p = a^{-i}b^p = b^{-p}b^p = e$. وهكذا فإننا وجدنا عنصراً c ، له الرتبة p بحيث إن $c \notin [a]$. ولأننا اخترنا b بحيث كان b له أصغر رتبة ، وكان $b \notin [a]$ ، فإننا نستنتج أن b له أيضاً الرتبة p ، ويكون ادعاؤنا قد تحقق .

والآن اعتبر زمرة القسمة $\overline{G} := G/[b]$. وليكن $\overline{x} := x[b]$ عنصراً فى $\overline{G}$. إذا كان $Ord(\overline{a}) < Ord(a) = p^m$ فإن $(\overline{a})^{p^{m-1}} = \overline{e}$ وهذا يعنى أن $(a[b])^{p^{m-1}} = a^{p^{m-1}}[b] = [b]$ ، بحيث إن : $a^{p^{m-1}} \in [a] \cap [b] = \{e\}$ وهذا يتناقض مع أن $Ord(a) = p^m$. وهكذا فإن $Ord(\overline{a}) = Ord(a) = p^m$ ومن ثم فإن $\overline{a}$ عنصر له أكبر رتبة فى $\overline{G}$. وبالاستقراء الرياضى نستطيع أن نكتب $\overline{G}$ بالشكل $[\overline{a}] \times \overline{K}$ لزمرة جزئية $\overline{K}$ من $\overline{G}$. والآن ليكن $K := \{x \in G \mid \overline{x} \in \overline{K}\}$ حيث $\begin{matrix} \rho : G \to \overline{G} \\ x \mapsto \overline{x} \end{matrix}$ هو الهومومورفيزم الطبيعى . نحن ندعى أن : $[a] \cap K = \{e\}$. وذلك لأنه إذا كان $x \in [a] \cap K$ فإن $\overline{x} \in [\overline{a}] \cap \overline{K} = \{\overline{e}\} = \{[b]\}$ ، وهذا معناه $x[b] = [b]$ وبالتالى فإن $x \in [b]$ ومن ثم فإن $x \in [a] \cap [b] = \{e\}$. وينتج من مناقشة الرتب أن $G = [a]K$(*) وبالتالى فإن $G = [a] \times K$ (حاصل الضرب الداخلى المباشر).

والآن من (٤-١-٥) وبالاستقراء الرياضى ينتج أن :

<u>٤-١-٦ تمهيدية</u> :

أى زمرة إبدالية منتهية لها رتبة هى قوة (أس) عدد أولى تكون حاصل ضرب داخلى (مباشر) من زمر دائرية .

والآن ماذا يتبقى لنا حتى يكتمل برهان النظرية الأساسية للزمر الإبدالية المنتهية ؟ إن النتيجة (٤-١-٤) تبرهن على أن الزمرة الإبدالية المنتهية G يمكن كتابتها على الصورة $G = G(p_1) \times G(p_2) \times \ldots \times G(p_n)$ حيث $G(p_i)$ هى زمرة لها رتبة هى قوة (أس)

عدد أولى. بينما التمهيدية (٤-١-٦) تعطينا المقولة أن كلاً من هذه العوامل هو حاصل ضرب داخلى مباشر لزمر دائرية رتبها قوى (أسس) أعداد أولية . وهذا يعنى أنه يتبقى فقط البرهنة على وحدانية هذه العوامل . الزمر $G(p_i)$ تتحدد وحدانيتها من G لأنها تشكل عناصر G التى رتبها قوى لـ p_i . وبالتالى فإنه يتبقى فقط البرهنة على أنه توجد طريقة وحيدة (بدون حساب الأيزومورفيزمات وترتيب العوامل (up to isomorphism and rearrangement of factors) لكتابة $G(p_i)$ كحاصل ضرب داخلى مباشر لزمر دائرية .

<u>٤-١-٧ تمهيدية</u> :

لتكن G زمرة إبدالية منتهية رتبتها قوة (أس) عدد أولى . إذا كانت

$$G = H_1 \times H_2 \times \ldots \times H_m = K_1 \times K_2 \times \ldots \times K_n$$

حيث $H's$ ، $K's$ زمر جزئية دائرية غير تافهة بحيث إن

$$Ord(K_1) \geq Ord(K_2) \geq \ldots \geq Ord(K_n) \quad \text{،} \quad Ord(H_1) \geq Ord(H_2) \geq \ldots \geq Ord(H_m)$$

فإن $m = n$ ، $Ord(H_i) = Ord(K_i)$ لجميع i .

<u>البرهان</u>: بالاستقراء الرياضى على $Ord(G)$. التقرير واضح فى حالة (عدد أولى) $Ord(G) = p$. لنفترض أن التقرير صحيح لجميع الزمر الإبدالية التى رتبتها أقل من $Ord(G)$. والآن لأى زمرة إبدالية L الزمرة : $L^p := \{x^p \mid x \in L\}$ هى زمرة جزئية من الزمرة L : لأن $e = e^p \in L^p$ أى أن $L^p \neq \phi$ ، وكذلك لأى $x^p, y^p \in L^p$:

(لأن L إبدالية ، $x, y \in L$) $x^p(y^p)^{-1} = x^p(y^{-1})^p = (xy^{-1})^p \in L^p$ ، والآن ينتج أن :

$$G^p = H_1^p \times H_2^p \times \ldots \times H_{m'}^p = K_1^p \times K_2^p \times \ldots \times K_{n'}^p$$

حيث m' أكبر عدد صحيح i بحيث إن $Ord(H_i) > p$ ، n' أكبر عدد صحيح j بحيث إن $Ord(K_j) > p$. (هذا يؤكد أن حاصل الضربين المباشرين الداخليين لـ G^p لايحتويان على عوامل تافهة). ونظراً لأن $Ord(G^p) < Ord(G)$ فمن الاستقراء الرياضى يكون لدينا

$m'=n'$ ، $Ord(H_i^p)=Ord(K_i^p)$ لجميع $i=1,2,...,m'$. ونظراً لأن $Ord(H_i)=pOrd(H_i^p)$ فإن $Ord(H_i)=Ord(K_i)$ لجميع $i=1,2,...,m'$.

يتبقى فقط البرهنة على أن عدد الـ H_i ذوات الرتبة p يساوى عدد الـ K_i ذوات الرتبة p . أى أن $m-m'=n-n'$ وهذا ينتج مباشرة من أن

$$Ord(H_1).Ord(H_2)...Ord(H_{m'})p^{m-m'}=Ord(G)$$

$$=Ord(K_1).Ord(K_2)...Ord(K_{n'})p^{n-n'}, Ord(H_i)=Ord(K_i)$$

أى أن $m-m'=n-n'$.

ومن حيث إن $m'=n'$ ينتج أن $m=n$.

٤-١-٨ : نظرية (بدون برهان)

إذا كانت A ، B ، C زمراً إبدالية وكانت A منتهية فإن :

$A\otimes B\cong A\otimes C$ (متشاكلتان) إذا كان وفقط إذا كان $B\cong C$.

٤-١-٩ امثلة :

مثال ١ : اكتب حواصل الضرب المباشرة الممكنة فى حالة إذا كانت رتبة الزمرة الإبدالية المنتهية هى :

(أ) 4 (ب) 8 (جـ) 16

الحــل :

(أ) $\mathbb{Z}_4$ أو $\mathbb{Z}_2\otimes\mathbb{Z}_2$

(ب) $\mathbb{Z}_8$ أو $\mathbb{Z}_2\otimes\mathbb{Z}_4$ أو $\mathbb{Z}_2\otimes\mathbb{Z}_2\otimes\mathbb{Z}_2$

(جـ) $\mathbb{Z}_{16}$ أو $\mathbb{Z}_2\otimes\mathbb{Z}_8$ أو $\mathbb{Z}_2\otimes\mathbb{Z}_2\otimes\mathbb{Z}_4$ أو $\mathbb{Z}_2\otimes\mathbb{Z}_2\otimes\mathbb{Z}_2\otimes\mathbb{Z}_2$ أو $\mathbb{Z}_4\otimes\mathbb{Z}_4$

مثال ٢: لتكن $G:=\{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ مع عملية الضرب مقياس 65 . عبر عن G بدلالة حاصلى الضرب الداخلى والخارجى المباشرين لزمر إبدالية منتهية .

الحل : سنكتب أولاً رتب عناصر G :

العنصر	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
الرتبة	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

(أ) كحاصل ضرب داخلى مباشر : سنختار عنصراً يكون ذا رتبة عظمى ، وليكن 8 . وبهذا يكون [8] عاملاً فى حاصل الضرب الداخلى . ثم نختار عنصراً آخر a بحيث تكون رتبة (a) هى 4 (لأن رتبة (G) هى 16 ، رتبة ([8]) هى 4) وبحيث يكون $a, a^2, a^3 \notin [8]$

({1, 8, 64, 57} = [18]) . 12 يحقق هذه الشروط ، وبهذا يكون : $G = [8] \times [12]$

(ب) كحاصل ضرب خارجى مباشر : الزمر الإبدالية التى رتبتها 16 هى :

$\mathbb{Z}_{16}, \mathbb{Z}_8 \otimes \mathbb{Z}_2, \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2, \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2, \mathbb{Z}_4 \otimes \mathbb{Z}_4$

$\mathbb{Z}_{16}$ مستبعدة لأن $1 \in \mathbb{Z}_{16}$ رتبته 16 ، G ليس بها عنصر رتبته 16 .

$\mathbb{Z}_8 \otimes \mathbb{Z}_2$ مستبعدة أيضاً لأن $(1,1) \in \mathbb{Z}_8 \otimes \mathbb{Z}_2$ رتبته 8 و G ليس بها عنصر رتبته 8

$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ مستبعدة لأنه لايوجد بها عنصر رتبته 4 ، بينما G بها 12 عنصراً من الرتبة 4 .

$\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ بها العناصر الآتية من الرتبة 4 :

(1, 0, 0), (1, 1, 0), (1, 0, 1), (1, 1, 1), (3, 0, 0), (3, 1, 0), (3, 0, 1), (3, 1, 1)

وهى ثمانية عناصر ، بينما G بها 12 عنصراً من الرتبة 4 . إذن هذه الحالة مستبعدة

$\mathbb{Z}_4 \otimes \mathbb{Z}_4$: جميع عناصرها من الرتبة 4 فيما عدا العناصر :

(0, 0), (0, 2), (2, 0), (2, 2)

إذن بها 12 عنصراً من الرتبة 4 ، وبها 3 عناصر من الرتبة 2 هى (0, 2) ، (2, 0) ، (2, 2)، وعنصر واحد من الرتبة 1 هو (0, 0) . وتكون متشاكلة مع G .

مثال ٣ : لتكن

$G := \{1, 8, 17, 19, 26, 28, 37, 44, 46, 63, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$

والعملية هى الضرب مقياس 135 (modulo) . عبر عن G كحاصل ضرب داخلى وخارجى مباشرين

الحـل : $8^3 = 512 \equiv 107 (\mathrm{mod}\, 135)$ ومن ثم فإن :

$$8^6 \equiv (107)^2 (\mathrm{mod}\, 135) \equiv 109 (\mathrm{mod}\, 135), 8^{12} \equiv (109)^2 (\mathrm{mod}\, 135) \equiv 1 (\mathrm{mod}\, 135)$$

كذلك فإن : $134 \equiv -1 (\mathrm{mod}\, 135)$ ومن ثم فإن $(134)^2 \equiv 1 (\mathrm{mod}\, 135)$ ، $(109)^2 \equiv 1 (\mathrm{mod}\, 135)$. أى أن $Ord(134) = Ord(109) = 2$

والآن G تكون متشاكلة مع إحدى الزمر :

$$\mathbb{Z}_{24} \cong \mathbb{Z}_8 \otimes \mathbb{Z}_3 \quad \text{or} \quad \mathbb{Z}_{12} \otimes \mathbb{Z}_2 \cong \mathbb{Z}_4 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_2 \quad \text{or}$$

$$\mathbb{Z}_6 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3$$

(راجع النتيجة (٣-١-١١))

رتبة (8) هى 12 تستبعد الزمرة الأخيرة لأنه لايوجد بها عنصر رتبة 12 . كذلك هناك عنصران فى G رتبتهما 2 بينما $\mathbb{Z}_{24}$ بها عنصر واحد رتبته 2 هو 12 . إذن G تكون متشاكلة مع $\mathbb{Z}_{12} \otimes \mathbb{Z}_2$.

أما بالنسبة لحاصل الضرب الداخلى المباشر فرتبة ([134]) هى 2 ، رتبة ([8]) هى 12

ملحوظة : لم نضع "−" فوق كل رقم فى المثالين السابقين للسهولة فى الكتابة .

كما أن $134 \notin [8]$ ، ورتبة (G) هى 24 ، ومن ثم فإن $G = [8] \times [134]$

مثال ٤ : اكتب $\mathbb{Z}_4 \otimes \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5$ على الشكل $\mathbb{Z}_{n_1} \otimes \mathbb{Z}_{n_2} \otimes ... \otimes \mathbb{Z}_{n_k}$ بحيث يكون n_i قاسما لـــ n_{i-1}

الحـل :

$$\mathbb{Z}_4 \otimes \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5 \cong \mathbb{Z}_4 \otimes \mathbb{Z}_9 \otimes \mathbb{Z}_5 \otimes \mathbb{Z}_4 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_2$$

$$\cong \mathbb{Z}_{180} \otimes \mathbb{Z}_{12} \otimes \mathbb{Z}_2$$

٤-١-١٠ نتيجة :

يستنتج من النظرية الأساسية للزمر الإبدالية أنه إذا كانت m تقسم رتبة زمرة إبدالية منتهية G ، فإن G لها زمرة جزئية رتبتها m .

٤-١-١١ مثال : G من الرتبة 72 وهى زمرة إبدالية . المطلوب الحصول على زمرة جزئية منها لها الرتبة 12 .

الحـل : وفقاً للنظرية الأساسية للزمر الإبدالية المنتهية تكون G متشاكلة مع إحدى الزمر:

$$\mathbb{Z}_8 \otimes \mathbb{Z}_9 \quad \text{or} \quad \mathbb{Z}_8 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \quad \text{or} \quad \otimes \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9 \quad \text{or} \quad \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$$

$$\text{or} \quad \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9 \quad \text{or} \quad \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$$

$\mathbb{Z}_8 \otimes \mathbb{Z}_9 \cong \mathbb{Z}_{72}$ (راجع (٣-١-١١)) ومن النتيجة السابقة تحتوى على زمرة جزئية رتبتها 12. $\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \cong \mathbb{Z}_{12} \otimes \mathbb{Z}_6$ (راجع (٣-١-١١)) وهى تحتوى كذلك على زمرة جزئية رتبتها 12 هى : $\{(\overline{0},\overline{0}),(\overline{1},\overline{0}),...,(\overline{11},\overline{0})\}$

وللحصول على زمرة جزئية رتبتها 12 من الزمرة $\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9$ نأخذ الزمرة :

$$\{(\overline{m},\overline{0},\overline{n}) \mid \overline{m} \in \mathbb{Z}_4, \overline{n}\{\overline{0},\overline{3},\overline{6}\}\}$$

وللحصول على زمرة جزئية رتبتها 12 من الزمرة $\mathbb{Z}_8 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$ نأخذ الزمرة :

$$\{(\overline{m},\overline{n},\overline{0}) \mid \overline{m} \in \{\overline{0},\overline{2},\overline{4},\overline{6}\}, \overline{n} \in \mathbb{Z}_3\}$$

ومن $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9$ نأخذ الزمرة :

$$\{(\overline{k},\overline{\ell},\overline{0},\overline{n}) \mid \overline{k},\overline{\ell} \in \mathbb{Z}_2, \overline{n} \in \{\overline{0},\overline{3},\overline{6}\}\}$$

ومن $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$ نأخذ الزمرة :

$$\{(\overline{k},\overline{\ell},\overline{0},\overline{0},\overline{p}) \mid \overline{k},\overline{\ell} \in \mathbb{Z}_2, \overline{p} \in \mathbb{Z}_3\}$$

٤-١-١٢ أمثلة متنوعة :

مثال ١ : ما أصغر عدد صحيح موجب n بحيث إنه يوجد بالضبط أربع زمر إبدالية غير متشاكلة من الرتبة n ؟

<u>الحـل</u> : $n = 36$ والزمر الأربع هى : $\mathbb{Z}_9 \otimes \mathbb{Z}_4$ ، $\mathbb{Z}_9 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ ، $\mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_4$ ، $\mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$.

<u>مثال ٢</u> : برهن على أنه فى أية زمرة إبدالية من الرتبة 45 يوجد عنصر رتبته 15 . هل تحتوى أية زمرة من الرتبة 45 عنصراً رتبته 9 ؟

<u>الحـل</u> :الزمر الإبدالية من الرتبة 45 هى : $\mathbb{Z}_{45} \cong \mathbb{Z}_5 \otimes \mathbb{Z}_9, \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5$. أى أنه بدون حساب التشاكلات (الأيزومورفيزمات) توجد فقط زمرتان إبداليتان لهما الرتبة 45 . واضح أنه فى الزمرة $\mathbb{Z}_5 \otimes \mathbb{Z}_9$ العنصر $(1,3)$ رتبته 15 ، وفى الزمرة $\mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5$ العنصر $(1, 1, 1)$ رتبته 15 (راجع (٣-١-٧)). الزمرة $\mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5$ ليس بها عنصر رتبته 9 .

<u>مثال ٣</u> : برهن على أنه توجد زمرتان إبداليتان من الرتبة 108 لكل منهما زمرة جزئية واحدة بالضبط من الرتبة 3

<u>البرهان</u> : الزمر الإبدالية من الرتبة 108 هى : $\mathbb{Z}_{108} \cong \mathbb{Z}_4 \otimes \mathbb{Z}_{27}$ ، $\mathbb{Z}_4 \otimes Z_3 \otimes \mathbb{Z}_9$ ، $\mathbb{Z}_4 \otimes Z_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$ ، $\mathbb{Z}_2 \otimes Z_2 \otimes \mathbb{Z}_{27}$ ، $\mathbb{Z}_2 \otimes Z_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_9$ ، $\mathbb{Z}_2 \otimes Z_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$.

الزمرة $\mathbb{Z}_4 \otimes Z_{27}$ بها زمرة جزئية واحدة من الرتبة 3 هى الزمرة المتولدة من العنصر $(\bar{0},\bar{9})$ أى هى :

$$[(\bar{0},\bar{9})] = \{(\bar{0},\bar{9}),(\bar{0},\overline{18}),(\bar{0},\bar{0})\}$$

الزمرة $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes Z_{27}$ بها زمرة جزئية واحدة من الرتبة 3 هى الزمرة المتولدة من العنصر $(\bar{0},\bar{0},\bar{9})$ أى هى :

$$[(\bar{0},\bar{0},\bar{9})] = \{(\bar{0},\bar{0},\bar{9}),(\bar{0},\bar{0},\overline{18}),(\bar{0},\bar{0},\bar{0})\}$$

<u>مثال ٤</u> : برهن على أنه توجد زمرتان إبداليتان من الرتبة 108 لكل منهما أربع زمر جزئية بالضبط من الرتبة 3 .

<u>البرهان</u> : بالنظر إلى المثال السابق مباشرة : الزمرة $\mathbb{Z}_4 \otimes \mathbb{Z}_3 \otimes Z_9$ لها الزمر الجزئية الآتية :

$[(\bar{0},\bar{0},\bar{3})] = \{(\bar{0},\bar{0},\bar{3}),(\bar{0},\bar{0},\bar{6}),(\bar{0},\bar{0},\bar{0})\}$,

$[(\bar{0},\bar{1},\bar{0})] = \{(\bar{0},\bar{1},\bar{0}),(\bar{0},\bar{2},\bar{0}),(\bar{0},\bar{0},\bar{0})\}$,

$[(\bar{0},\bar{1},\bar{3})] = \{(\bar{0},\bar{1},\bar{3}),(\bar{0},\bar{2},\bar{6}),(\bar{0},\bar{0},\bar{0})\}$,

$[(\bar{0},\bar{2},\bar{3})] = \{(\bar{0},\bar{2},\bar{3}),(\bar{0},\bar{1},\bar{6}),(\bar{0},\bar{0},\bar{0})\}$

والزمرة : $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes Z_9$ لها الزمر الجزئية الآتية :

$[(\bar{0},\bar{0},\bar{0},\bar{3})] = \{(\bar{0},\bar{0},\bar{0},\bar{3}),(\bar{0},\bar{0},\bar{0},\bar{6}),(\bar{0},\bar{0},\bar{0},\bar{0})\}$

$[(\bar{0},\bar{0},\bar{1},\bar{0})] = \{(\bar{0},\bar{0},\bar{1},\bar{0}),(\bar{0},\bar{0},\bar{2},\bar{0}),(\bar{0},\bar{0},\bar{0},\bar{0})\}$

$[(\bar{0},\bar{0},\bar{1},\bar{3})] = \{(\bar{0},\bar{0},\bar{1},\bar{3}),(\bar{0},\bar{0},\bar{2},\bar{6}),(\bar{0},\bar{0},\bar{0},\bar{0})\}$

$[(\bar{0},\bar{0},\bar{1},\bar{6})] = \{(\bar{0},\bar{0},\bar{1},\bar{6}),(\bar{0},\bar{0},\bar{2},\bar{3}),(\bar{0},\bar{0},\bar{0},\bar{0})\}$

<u>مثال ٥</u> : لتكن G زمرة إبدالية من الرتبة 120 ، لها بالضبط 3 عناصر من الرتبة 2 . عين فصل أو فصول التشاكل لـــ G

<u>الحــل</u> : إذا كانت G زمرة إبدالية من الرتبة 120 فإن فصول التشاكل لها هى :

$$\mathbb{Z}_8 \otimes \mathbb{Z}_{15} \ , \ \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_{15} \ , \ \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_{15}$$

واضح أن الزمرة $\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_{15}$ هى الزمرة المعنية فعناصرها ذوات الرتبة الثانية هى :

$$(\bar{2},\bar{1},\bar{0}) \ \text{،} \ (\bar{2},\bar{0},\bar{0}) \ \text{،} \ (\bar{0},\bar{1},\bar{0})$$

<u>مثال ٦</u> : بدون حساب التشاكلات (الأيزومورفيزمات) (up to isomorphism) اوجد جميع الزمر الإبدالية من الرتبة 360 .

<u>الحــل</u> : $360 = 5 \times 8 \times 9$ وبهذا تكون الزمر الإبدالية هى :

$$\mathbb{Z}_5 \otimes \mathbb{Z}_8 \otimes \mathbb{Z}_9 \ , \ \mathbb{Z}_5 \otimes \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9 \ , \ \mathbb{Z}_5 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9,$$

$$\mathbb{Z}_5 \otimes \mathbb{Z}_8 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \ , \ \mathbb{Z}_5 \otimes \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \ , \ \mathbb{Z}_5 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$$

مثال ٧ : برهن بضرب مثال على أنه إذا كانت رتبة زمرة إبدالية تقبل القسمة على 4 ، فليس بالضرورة أن تحتوى الزمرة على زمرة جزئية دائرية من الرتبة 4 .

البرهان : الزمرة $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ ليست دائرية ولا تحتوى على زمرة جزئية دائرية من الرتبة 4 .

مثال ٨ : كم عدد الزمر الإبدالية التي لها الرتب الآتية(بدون حساب الأيزومورفيزمات) :

(أ) 6 (ب) 15 (جـ) 42 (د) pq حيث p، q عددان أوليان مختلفان

(هـ) $p\,q\,r$ حيث p ، q ، r أعداد أولية مختلفة (و) عمم النتائج السابقة

الحــل : (أ) لدينا $\mathbb{Z}_6 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_3$ وهى الوحيدة

(ب) $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \otimes \mathbb{Z}_5$ وهى كذلك الوحيدة

(جـ) $\mathbb{Z}_{42} \cong \mathbb{Z}_6 \otimes \mathbb{Z}_7 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_7$ وهى كذلك الوحيدة

(د) $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \otimes \mathbb{Z}_q$ وهى الوحيدة

(هـ) $\mathbb{Z}_{pqr} \cong \mathbb{Z}_p \otimes \mathbb{Z}_q \otimes \mathbb{Z}_r$ وهى الوحيدة

(و) يكون لدينا زمرة إبدالية وحيدة من الرتبة n إذا كان وفقط إذا كان ليس من عوامل n أى مربع لعدد أولى .

مثال ٩: حقق النتيجة (٤-١-١٠) فى حالة إذا ما كانت رتبة الزمرة هى 1080 ، وكـــان القاسم هو 180

الحــل : $1080 = 8\times27\times5$ وبالتالى فإن الزمر الإبدالية من الرتبة 1080 (بدون حساب الأيزومورفيزمات) هى :

$$\mathbb{Z}_{1080} \cong \mathbb{Z}_8 \otimes \mathbb{Z}_{27} \otimes \mathbb{Z}_5,\ \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_{27} \otimes \mathbb{Z}_5\ ,\ \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_{27} \otimes \mathbb{Z}_5,$$

$$\mathbb{Z}_8 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_9 \otimes \mathbb{Z}_5\ ,\ \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_9 \otimes \mathbb{Z}_5\ ,\ \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_9 \otimes \mathbb{Z}_5,$$

$$\mathbb{Z}_8 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5\ ,\ \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5\ ,$$

$$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_5\ .$$

لإيجاد زمر جزئية رتبها 60 ، 30 ، 540 ، 216 :

$\mathbb{Z}_8 \otimes \mathbb{Z}_{27} \otimes \mathbb{Z}_5$ تحتوى على الزمرة الجزئية $[(\bar{2},\bar{9},\bar{1})]$ التى رتبتها $4\times3\times5$

$\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_{27} \otimes \mathbb{Z}_5$ تحتوى على الزمرة الجزئية $[(\bar{0},\bar{1},\bar{9},\bar{1})]$ التى رتبتها $1\times2\times3\times5$

$\mathbb{Z}_8 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_9 \otimes \mathbb{Z}_5$ تحتوى على الزمرة الجزئية $[(\bar{2},\bar{1},\bar{1},\bar{1})]$ التى رتبتها $4\times3\times9\times5$

$\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_9 \otimes \mathbb{Z}_5$ تحتوى على الزمرة الجزئية $[(\bar{1},\bar{1},\bar{1},\bar{1},\bar{0})]$ التى رتبتها $4\times2\times3\times9\times1$.

وبالمثل لأى رتب أخرى .

مثال ١٠ : فى مثال ٢ من (٤-١-٩) وضح لماذا يمكن الاستغناء عن حساب رتب الخمسة عناصر الأخيرة حتى نعبر عن G كحاصل ضرب خارجى مباشر .

الحـــل : رتب العناصر الخمسة الأخيرة لن تضيف شيئاً ، لأن عدد العناصر التى رتبتها 4 فى الأحد عشرعنصراً الأولى هو 9 وأكبر عدد من العناصر التى رتبتها 4 فى الزمر الإبدالية من الرتبة 16 هو 8 باستثناء الزمرة $\mathbb{Z}_4 \otimes \mathbb{Z}_4$ التى تكون بالضرورة متشاكلة مع الزمرة المعطاة G .

مثال ١١ : برهن على أن أى زمرة إبدالية ذات رتبة فردية لايمكن أن تحتوى على عنصر ذى رتبة زوجية .

الحـــل : سواء كانت الزمرة إبدالية أم كانت غير إبدالية فإنه من النتيجة (١-١١-٩) بشقيها (١) ، (٢) ينتج أن رتبة أى عنصر فى زمرة تقسم رتبة الزمرة وبالتالى فلا يمكن أن ينتمى عنصر ذو رتبة زوجية إلى زمرة ذات رتبة فردية .

طريقة أخرى: استخدم النظريات: (١-١٠-٣) لاجرانج ، (١-١١-٧)(١٤)، (٣-١-٧)، (٤-١-١) (النظرية الأساسية للزمر الإبدالية المنتهية) .

مثال ١٢ : لتكن G زمرة إبدالية من الرتبة 9 . ما أكبر عدد من العناصر (فيما عدا عنصر الوحدة) التى يجب أن نحسب رتبتها حتى نعين فصل التشاكل لـــ G ؟ ماذا لو كانت رتبة G هى ١٨ ؟

الحـــل : فصول التشاكل فى حالة الرتبة 9 فصلان : (أ) $\mathbb{Z}_9$ (ب) $\mathbb{Z}_3 \otimes \mathbb{Z}_3$

نحتاج فى الواقع إلى معرفة رتب أربعة عناصر بما فيها عنصر الوحدة (أى رتب ثلاثة عناصر باستبعاد عنصر الوحدة). ولبيان ذلك نحسب الرتب فى الحالتين(أ)،(ب) للعناصر:

(أ) العنصران $\bar{3}$، $\bar{6}$ لهما الرتبة 3 . العنصر $\bar{0}$ له الرتبة1 . باقى العناصر لها الرتبة 9.

(ب) جميع العناصر لها الرتبة 3 ، فيما عدا عنصر الوحدة $(\bar{0},\bar{0})$ له الرتبة 1 .

بمعرفة رتب أربعة عناصر بما فيها عنصر الوحدة لدينا الحالات الآتية :

(١) لايوجد رتبة 3 على الإطلاق : إذن G من الفصل (أ)

(٢) يوجد ثلاثة عناصر من غير الرتبة 3 ، عنصر من الرتبة 3 : G من الفصل (أ)

(٣) يوجد عنصران من غير الرتبة 3 ، عنصران من الرتبة 3 : G من الفصل (أ)

(٤) يوجد عنصر واحد من غير الرتبة 3 ، ثلاثة عناصر من الرتبة 3:G من الفصل (ب)

(٥) جميع العناصر من الرتبة 3 : G من الفصل (ب)

قد يحدث أن نكتشف فصل التشاكل بمعرفة عدد من الرتب أقل من 4 (بما فيها رتبة عنصر الوحدة) فإذا كان – مثلاً– لدينا رتبتان فقط لاتساويان 3 فإن G تكون من الفصل (أ) ولانحتاج لمعرفة رتبتين أخريين .

فى حالة الرتبة 18 سنكتب فصول التشاكل لـــ G : فصلان :

(أ) $\mathbb{Z}_{18} \cong \mathbb{Z}_2 \otimes \mathbb{Z}_9$ وعناصر $\mathbb{Z}_2 \otimes \mathbb{Z}_9$ هى :

$$(\bar{0},\bar{0}),(\bar{0},\bar{1}),\ldots,(\bar{0},\bar{8}),(\bar{1},\bar{0}),(\bar{1},\bar{1}),\ldots,(\bar{1},\bar{8})$$

عناصر $\mathbb{Z}_{18}$ التى لها الرتبة 18 ستة عناصر هى : $\bar{1}$ ، $\bar{5}$ ، $\bar{7}$ ، $\overline{11}$ ، $\overline{13}$ ، $\overline{17}$ ؛

والتى لها الرتبة 9 ستة عناصر هى : $\bar{2}$ ، $\bar{4}$ ، $\bar{8}$ ، $\overline{10}$ ، $\overline{14}$ ، $\overline{16}$ ؛

واللذان لهما الرتبة 6 هما : $\bar{3}$ ، $\overline{15}$ ؛ واللذان لهما الرتبة 3 هما : $\bar{6}$ ، $\overline{12}$

والذى له الرتبة 2 هو $\bar{9}$ والذى له الرتبة 1 هو $\bar{0}$.

(ب) $\mathbb{Z}_3 \otimes \mathbb{Z}_6 \cong \mathbb{Z}_3 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_2$ وعناصر $\mathbb{Z}_3 \otimes \mathbb{Z}_6$ ورتبها هى :

العنصر	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{0},\bar{3})$	$(\bar{0},\bar{4})$	$(\bar{0},\bar{5})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$
الرتبة	1	6	3	2	3	6	3	6	3

العنصر	$(\bar{1},\bar{3})$	$(\bar{1},\bar{4})$	$(\bar{1},\bar{5})$	$(\bar{2},\bar{0})$	$(\bar{2},\bar{1})$	$(\bar{2},\bar{2})$	$(\bar{2},\bar{3})$	$(\bar{2},\bar{4})$	$(\bar{2},\bar{5})$
الرتبة	6	3	6	3	6	3	6	3	6

أى أن عدد العناصر التى رتبتها 6 هى ثمانية ، وعدد العناصر التى رتبتها 3 هى ثمانية وعنصر واحد رتبته اثنان وعنصر واحد رتبته واحد .

إذا علمنا رتب سبعة عناصر ولم يكن من بينها الرتبة 18 أو الرتبة 9 كانت G لها فصل التشاكل $\mathbb{Z}_3 \otimes \mathbb{Z}_6$. أما إذا ظهرت الرتبة 18أو الرتبة 9 فمعنى هذا أن G لها فصل التشاكل $\mathbb{Z}_{18}$ ، أى أننا احتجنا إلى معرفة رتبة ستة عناصر بخلاف رتبة عنصر الوحدة $(\bar{0},\bar{0})$.

وقد يحدث أن نكتشف فصل التشاكل قبل أن نعرف رتبة كل هذه العناصر إذا ظهرت الرتبة 18 أو الرتبة 9 قبل ذلك .

<u>مثال ١٣</u> : لتكن G زمرة إبدالية من الرتبة 16 ، بها عنصران a ، b بحيث تكون $Ord(a)=4=Ord(b)$ ، $a^2 \neq b^2$. عين فصل تشاكل G .

<u>الحـــل</u> : G لها فصول التشاكل الآتية : $\mathbb{Z}_{16}$ ، $\mathbb{Z}_8 \otimes \mathbb{Z}_2$ ، $\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ ، $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ ، $\mathbb{Z}_4 \otimes \mathbb{Z}_4$

$(\bar{1},\bar{0}),(\bar{1},\bar{1}) \in \mathbb{Z}_4 \otimes \mathbb{Z}_4$ ، $Ord(\bar{1},\bar{0})=4=Ord(\bar{1},\bar{1})$ ، $(\bar{1},\bar{0})+(\bar{1},\bar{0})=(\bar{2},\bar{0})$ بينما $(\bar{1},\bar{1})+(\bar{1},\bar{1})=(\bar{2},\bar{2})$ (لاحظ أن العملية هى الجمع مقياس 4) وبالتالى يكون فصل التشاكل للزمرة G هو $\mathbb{Z}_4 \otimes \mathbb{Z}_4$

<u>مثال ١٤</u>: كم عدد الزمر الإبدالية (بدون حساب الأيزومورفيزمات up to isomorphism) التى من الرتبة 24 ؟ من الرتبة 25 ؟ ومن الرتبة (25)(24) ؟

<u>الحـــل</u> : فصول التشاكل لزمرة إبدالية من الرتبة 24 هى : $\mathbb{Z}_{24}$ ، $\mathbb{Z}_4 \otimes \mathbb{Z}_6$ ، $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_6$. لاحظ أن $\gcd(2, 3) = 1$ ، كذلك لاحظ أن $\mathbb{Z}_2 \otimes \mathbb{Z}_{12} \cong \mathbb{Z}_4 \otimes \mathbb{Z}_6$ لأن كلتا الزمرتين تتشاكل مع الزمرة $\mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_4$. إذن هناك 3 زمر إبدالية من الرتبة 24 .

فصلا التشاكل لزمرة إبدالية من الرتبة 25 هما : $\mathbb{Z}_{25}$ ، $\mathbb{Z}_5 \otimes \mathbb{Z}_5$ ، أى هناك زمرتان إبداليتان من الرتبة 25 .

وبالتالى يكون هناك 6 زمر إبدالية من الرتبة (25)(24). [لاحظ أن $1 = (24, 25)$ (gc$d$)].

مثال ١٥ : كم عدد (بدون حساب الأيزومورفيزمات) الزمر الإبدالية من الرتبة 10^5 ؟

الحـل : $10^5 = (2^5)(5^5)$. فصول التشاكل للزمرة الإبدالية من الرتبة 2^5 هى :

$\mathbb{Z}_{2^5}$ ، $\mathbb{Z}_{2^4} \otimes \mathbb{Z}_2$ ، $\mathbb{Z}_{2^3} \otimes \mathbb{Z}_{2^2}$ ، $\mathbb{Z}_{2^2} \otimes \mathbb{Z}_{2^2} \otimes \mathbb{Z}_2$ ، $\mathbb{Z}_{2^2} \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ ،

$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ ، $\mathbb{Z}_{2^3} \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$: أى سبعة فصول تشاكل وبالمثل فإن فصول التشاكل للزمرة الإبدالية من الرتبة 5^5 هى :

$\mathbb{Z}_{5^5}$ ، $\mathbb{Z}_{5^4} \otimes \mathbb{Z}_5$ ، $\mathbb{Z}_{5^3} \otimes \mathbb{Z}_{5^2}$ ، $\mathbb{Z}_{5^2} \otimes \mathbb{Z}_{5^2} \otimes \mathbb{Z}_5$ ، $\mathbb{Z}_{5^2} \otimes \mathbb{Z}_5 \otimes \mathbb{Z}_5 \otimes \mathbb{Z}_5$ ،

$\mathbb{Z}_5 \otimes \mathbb{Z}_5 \otimes \mathbb{Z}_5 \otimes \mathbb{Z}_5 \otimes \mathbb{Z}_5$ ، $\mathbb{Z}_{5^3} \otimes \mathbb{Z}_5 \otimes \mathbb{Z}_5$: أى سبعة فصول تشاكل ويكون – كما سبق فى مثال ١٤– هناك $7^2 = 49$ زمرة إبدالية من الرتبة10^5(بدون حساب الأيزومورفيزمات)

ملحوظة : لاحظ أن $\gcd(2^5,5^5)=1$ كما كانت الحال فى مثال ١٤ $\gcd(24,25)=1$.

ماذا يحدث لو لم يكن القاسم المشترك الأعظم للرتبتين = 1 ؟

مثال ١٦ : اوجد الزمر الجزئية فى $\mathbb{Z}_{12}$ التى تتولد من $\{\bar{2},\bar{3}\}$ ، من $\{\bar{4},\bar{6}\}$ ، من $\{\bar{8},\bar{6},\overline{10}\}$.

الحـل : $\bar{1}=\bar{3}-\bar{2}$. إذن الزمرة الجزئية التى تتولد من $\{\bar{2},\bar{3}\}$ فى $\mathbb{Z}_{12}$ هى $\mathbb{Z}_{12}$ نفسها .

$\bar{2}=\bar{6}-\bar{4}$. واضح أن الزمرة الجزئية المتولدة فى هذه الحالة هى $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\}$ أى هى $[\bar{2}]$

كذلك الزمرة الجزئية المتولدة من $\{\bar{8},\bar{6},\overline{10}\}$ هى $[\bar{2}]$

مثال ١٧ : لتكن G زمرة إبدالية لها الرتبة 72 .

(أ) هل تستطيع القول بعدد الزمر الجزئية من G التى لها الرتبة 8 ؟ ولماذا ؟

(ب) هل تستطيع القول بعدد الزمر الجزئية من G التى لها الرتبة 4 ؟ ولماذا ؟

الحـل : فصول التشاكل لـــ G هى : $\mathbb{Z}_{72} \cong \mathbb{Z}_8 \otimes \mathbb{Z}_9$ ،

$\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$ ، $\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9$

$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$ $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9$

(أ) نعم نستطيع القول بأن عدد الزمر الجزئية من G التى لها الرتبة 8 هو الواحد ، أى زمرة جزئية واحدة نميزها بأن رتبة عناصرها تقسم رتبة الزمرة الجزئية أى تقسم 8 .

فإذا اعتبرنا $G = \mathbb{Z}_{72} = \mathbb{Z}_8 \otimes \mathbb{Z}_9$ فإن الزمرة الجزئية المعنية تكون هى $\mathbb{Z}_8 \otimes \{\bar{0}\}$

أما إن كانت $G = \mathbb{Z}_{72} = \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9$ فإن الزمرة الجزئية المعنية تكون هى

$\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \{\bar{0}\}$

أما إن كانت $G = \mathbb{Z}_{72} = \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9$ فإن الزمرة الجزئية المعنية تكون هى

$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \{\bar{0}\}$

أما إن كانت $G = \mathbb{Z}_{72} = \mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$ فإن الزمرة الجزئية المعنية تكون هى

$\mathbb{Z}_4 \otimes \mathbb{Z}_2 \otimes \{\bar{0}\} \otimes \{\bar{0}\}$

أما إن كانت $G = \mathbb{Z}_{72} = \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_3 \otimes \mathbb{Z}_3$ فإن الزمرة الجزئية المعنية تكون هى $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \{\bar{0}\} \otimes \{\bar{0}\}$

وفى كل الحالات تكون هناك زمرة جزئية واحدة لها الرتبة 8 ، كما سبق

(ب) لانستطيع . فإذا اعتبرنا G هى $\mathbb{Z}_8 \otimes \mathbb{Z}_9$ فإنه توجد زمرة جزئية واحدة رتبتها 4 هى: $\{(\bar{a}, \bar{0}) \mid \bar{a} \in \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}\}$. أما إذا اعتبرنا G هى $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_9$ ففى هذه الحالة توجد سبع زمر جزئية رتبتها 4 هى :

1) {(1, 0, 0, 0), (0, 1, 0, 0), (1, 1, 0, 0), (0, 0, 0, 0)},

2) {(1, 0, 0, 0), (0, 0, 1, 0), (1, 0, 1, 0), (0, 0, 0, 0)},

3) {(0, 1, 0, 0), (0, 0, 1, 0), (0, 1, 1, 0), (0, 0, 0, 0)},

4) {(1, 1, 0, 0), (1, 0, 1, 0), (0, 1, 1, 0), (0, 0, 0, 0)},

5) {(1, 0, 0, 0), (0, 1, 1, 0), (1, 1, 1, 0), (0, 0, 0, 0)},

6) {(0, 1, 0, 0), (1, 0, 1, 0), (1, 1, 1, 0), (0, 0, 0, 0)},

7) {(0, 0, 1, 0), (1, 1, 0, 0), (1, 1, 1, 0), (0, 0, 0, 0)}

(ملحوظة : لم نضع "ــ" فوق كل رقم فيما سبق للسهولة فى الكتابة)

مثال ١٨ : ما أقل عدد من العناصر التى تولد $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ ؟

الحــل :

$$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2 = \{(\bar{0},\bar{0},\bar{0}),(\bar{0},\bar{0},\bar{1}),(\bar{0},\bar{1},\bar{0}),(\bar{1},\bar{0},\bar{0}), (\bar{0},\bar{1},\bar{1}),(\bar{1},\bar{0},\bar{1}),(\bar{1},\bar{1},\bar{0}),(\bar{1},\bar{1},\bar{1})\}$$

المجموعة $\{(\bar{1},\bar{0},\bar{0}),(\bar{0},\bar{1},\bar{0}),(\bar{0},\bar{0},\bar{1})\}$ تولد $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ ، وأقل عدد من العناصر تولد الزمرة المعطاة هو 3 .

مثال ١٩ : قرر إذا ما كانت التقريرات الآتية صائبة أم خاطئة :

(أ) كل زمرة إبدالية رتبتها عدد أولى تكون دائرية

(ب) كل زمرة إبدالية رتبتها قوة (أس) عدد أولى تكون دائرية

(جـ) $\mathbb{Z}_8$ تتولد من $\{\bar{4},\bar{6}\}$

(د) $\mathbb{Z}_8$ تتولد من $\{\bar{4},\bar{5},\bar{6}\}$

(هـ) كل زمرة إبدالية رتبتها تقبل القسمة على5 تحتوى على زمرة جزئية دائرية رتبتها5

(و) كل زمرة إبدالية رتبتها تقبل القسمة على6 تحتوى على زمرة جزئية دائرية رتبتها6

الحــل : (أ) صائب سواء علمنا أن كانت الزمرة إبدالية أو لم نعلم ستكون دائرية وبالتالى تكون إبدالية (نظرية (١-١١-٧) (٢))

(ب) خاطئ مثال مضاد : $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ رتبتها 4 وهى إبدالية ، لكنها ليست دائرية .

(جـ) خاطئ $[\{\bar{4},\bar{6}\}] = \{\bar{0},\bar{2},\bar{4},\bar{6}\} \neq \mathbb{Z}_8$

(د) صائب : $\bar{1} = \bar{5} - \bar{4}$ وهو مولد لـــ $\mathbb{Z}_8$

(هـ) ، (و) صائبان

تمارين

(١) يقال لزمرة G إنها **زمرة التواء** (torsion group) إذا كان كل عنصر من عناصرها له رتبة منتهية (finite order) . ويقال إنها خالية من الالتواء (torsion free) إذا كان عنصرها المحايد هو الوحيد الذى له رتبة منتهية .

برهن على أنه فى زمرة إبدالية G مجموعة العناصر التى لها رتب منتهية تكون زمرة جزئية من G (تسمى هذه الزمرة الجزئية زمرة الالتواء الجزئية فى G The torsion subgroup) .

(٢) برهن على أن $\{(1,\bar{0}),(0,\bar{1})\}$ مجموعة مولدة لـــ $\mathbb{Z}\otimes\mathbb{Z}_2$

(٣) برهن على أن كل زمرة منتهية تكون زمرة التواء ، بينما $(\mathbb{Z},+)$ خالية من الالتواء

(٤) اوجد زمرة الالتواء الجزئية من الزمرة $\mathbb{Z}\otimes\mathbb{Z}_2$

(٥) بدون حساب الأيزومورفيزمات اوجد جميع الزمر الإبدالية من الرتبة 720

(٦) اوجد رتب زمر الالتواء الجزئية فى $\mathbb{Z}_4\otimes\mathbb{Z}\otimes\mathbb{Z}_3$ ، $\mathbb{Z}_{12}\otimes\mathbb{Z}\otimes\mathbb{Z}_2$

(٧) اوجد زمرة الالتواء الجزئية فى الزمرة $(\mathbb{C}\setminus\{0\},.)$

(٨) ما أصغر عدد صحيح موجب n بحيث توجد زمرتان إبداليتان غير متشاكلتين من الرتبة n ؟

(٩) ما أصغر عدد صحيح موجب n بحيث توجد ثلاث زمر إبدالية غير متشاكلة من الرتبة n ؟

(١٠) برهن على أنه توجد زمرتان إبداليتان من الرتبة 108 لكل منهما 13 زمرة جزئية بالضبط من الرتبة 3

(١١) بدون حساب الأيزومورفيزمات قارن بين عدد الزمر الإبدالية من الرتبة m بتلك التى من الرتبة n إذا كان :

(أ) $n=3^2$ ، $m=5^2$

(ب) $n=2^4$ ، $m=5^4$

(جـ) $n = p^r$ ، $m = q^r$ حيث p ، q عددان أوليان مختلفان

(د) $n = p^r$ ، $m = p^r q$ حيث p ، q عددان أوليان مختلفان

(هـ) $n = p^r$ ، $m = p^r q^2$ حيث p ، q عددان أوليان مختلفان

(١٢) هل تشاكل زمرة تماثلات المستطيل (زمرة كلاين الرباعية) $\mathbb{Z}_4$ أم $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ ؟

(١٣) المجموعة $\{\bar{1}, \bar{9}, \overline{16}, \overline{22}, \overline{29}, \overline{53}, \overline{74}, \overline{79}, \overline{81}\}$ تكون زمرة مع الضرب مقياس 91 . عين فصل التشاكل لها

(١٤) عين الأعداد الصحيحة n بحيث تكون الزمر الإبدالية من الرتبة n دائرية

(١٥) عين الأعداد الصحيحة n بحيث تكون الزمر الإبدالية من الرتبة n لها أربعة فصول تشاكل بالضبط

(١٦) لتكن $G := \{\bar{1}, \bar{7}, \overline{17}, \overline{23}, \overline{49}, \overline{55}, \overline{65}, \overline{71}\}$ مع عملية الضرب مقياس 96 . عبر عن G كحاصلى ضرب مباشرين خارجي وداخلى من زمر دائرية

(١٧) لتكن $G := \{\bar{1}, \bar{7}, \overline{43}, \overline{49}, \overline{51}, \overline{57}, \overline{93}, \overline{99}, \overline{101}, \overline{107}, \overline{143}, \overline{149}, \overline{151}, \overline{157}, \overline{193}, \overline{199}\}$ مع عملية الضرب مقياس 200 . عبر عن G كحاصلى ضرب مباشرين خارجي وداخلى من زمر دائرية

(١٨) المجموعة $G := \{\bar{1}, \bar{4}, \overline{11}, \overline{14}, \overline{16}, \overline{19}, \overline{26}, \overline{29}, \overline{31}, \overline{34}, \overline{41}, \overline{44}\}$ تكون زمرة مع عملية الضرب مقياس 45 . عبر عن G كحاصلى ضرب مباشرين خارجي وداخلى من زمر دائرية ذات رتب قوى (أسس) أعداد أولية .

(١٩) لتكن G زمرة إبدالية من الرتبة 16 . ما أكبر عدد من العناصر (فيما عدا عنصر الوحدة) التى تحتاج إلى حساب رتبتها حتى نعين فصل التشاكل لـــ G .

(٢٠) فى التمهيدية (٤-١-٥) برهن على صحة العبارة (*) : " وينتج من مناقشة الرتب أن $G = [a]K$ "

1 Group Theory نظرية الزمر

القسم



The Sylow Theorems نظريات سيلو

٥-١ عمل زمرة على مجموعة The action of a group on a set

٥-١-١ تعريف : يقال لزمرة G إنها تعمل على مجموعة (act on a set S) S إذا كان هناك راسم من $G\times S$ إلى S (يعبر عنه عادة بـ $(g,x)\mapsto gx$) بحيث إنه لكل $x\in S$ ولكل $g_1,g_2\in G$:

$$ex=x, \quad (g_1g_2)x=g_1(g_2x)$$

(حيث e العنصر المحايد فى G)

٥-١-٢ أمثلة : (يمكن التحقق منها مباشرة)

مثال ١ : الزمرة المتماثلة $\gamma_n(=S_n)$ تعمل على المجموعة $\{1, 2, \ldots, n\}$ كالآتى :

$$(\sigma,x)\mapsto\sigma(x) \quad , \quad \sigma\in\gamma_n,\ x\in\{1,2,\ldots,n\}$$

مثال ٢ : لتكن G زمرة ، H زمرة جزئية منها . H كزمرة تعمل على G كمجموعة كالآتى : $(h,x)\mapsto hx$ حيث hx هو "الضرب" فى G. يسمى عمل $h\in H$ على G نقلا (أيسر) ((left) translation) . وإذا كانت K زمرة جزئية أخرى من G ، وكانت S هى مجموعة جميع المجموعات المشاركة اليسرى من G بالنسبة إلى K فإن H تعمل على S بالنقل : $(h,xK)\mapsto hxK$.

مثال ٣ : لتكن H زمرة جزئية من زمرة G. H تعمل كزمرة علىG كمجموعة كالآتى : $(h,x)\mapsto hxh^{-1}$. التحقق :

$$(e,x)\mapsto exe^{-1}=x,$$

$$(h_1h_2,x)\mapsto h_1h_2xh_2^{-1}h_1^{-1}=h_1(h_2xh_2^{-1})h_1^{-1}\leftarrow\!\!\dashv h_1(h_2,x)$$

يسمى هذا العمل ترافقاً بـ h (conjugation by h) ، ويسمى العنصر hxh^{-1} ترافقاً لـ x (conjugation of x) (انظر (٢-١-٧))

وإذا كانت K زمرة جزئية من G وكانت $h\in H$ فإنه من السهل التحقق من أن hKh^{-1} تكون زمرة جزئية من G ومتشاكلة (أيزومورفية) مع K . ومن ثم فإن H تعمل على S

مجموعة كل الزمر الجزئية لـــ G بالترافق $(h,K)\mapsto hKh^{-1}$. **ويقال إن الزمرة** hKh^{-1} **ترافق K** (to be conjugate to K)

٥-١-٣ نظرية : إذا كانت G زمرة تعمل على مجموعة S فإن :

(أ) العلاقة على S المعرفة كالآتى :

$$x \sim x' \Leftrightarrow gx = x'$$

لبعض $g\in G$ (for some $g\in G$) تكون علاقة تكافؤ .

(ب) لكل $x\in S$:

$$G_x := \{g\in G \mid gx = x\}$$

زمرة جزئية من G .

البرهان : (أ) انعكاسية (reflexive) $\forall x\in S:\ ex = x \ \Rightarrow x\sim x \ \Rightarrow \ \sim$

$$x\sim x' \Rightarrow \exists g\in G: gx = x' \Rightarrow x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x', g^{-1}\in G$$

$\Rightarrow \ \sim$ متناظرة (متماثلة symmetric)

$$x\sim x', x'\sim x'' \Rightarrow \exists g_1, g_2\in G: g_1x = x', g_2x' = x'' \Rightarrow (g_2g_1)x$$

$= g_2(g_1x) = x'', g_2g_1\in G \Rightarrow \ \sim$ (transitive)انتقالية

$\Rightarrow \sim$ (equivalence relation) علاقة تكافؤ

(ب) $e\in G_x$ (العنصر المحايد فى G) لأن $ex = x$ أى أن $G_x\neq\phi$. ليكن $g_1, g_2\in G_x$

ينتج أن : $g_1x = x$ ، $g_2x = x$. وبالتالى فإن : $g_2x = g_1x$

ومن ثم فإن : $(g_2^{-1}g_1)x = g_2^{-1}(g_1x) = x$ ، $g_2^{-1}g_1\in G$ وبالتالى فإن $g_2^{-1}g_1\in G_x$.

وينتج المطلوب مباشرة .

٥-١-٤ تعريف : فصول التكافؤ (The equivalence classes) لعلاقة التكافؤ المعرفة فى (٥-١-٣(أ)) تسمى **مسارات** G (orbits) على S ، ويشار إلى مسار $S\ni x$ بالرمز $\overline{x}$. وتسمى الزمرة الجزئية G_x فى (٥-١-٣ (ب)) فى مواطن كثيرة **الزمرة الجزئية المثبتة x** (The subgroup fixing x) أو **زمرة توحيد الخواص لـــ x** (The isotropy group of x) أو **موازن x** (stabilizer of x) .

وأذا كانت الزمرة G تعمل على نفسها بالترافق (by conjugation) عندئذ يسمى المسار لـ x: $\{gxg^{-1} \mid g \in G\}$ **بفصل الترافق لـ x** (conjugacy class of x)

٥-١-٥ أمثلة : إذا كانت الزمرة الجزئية H تعمل على الزمرة G بالترافق فإن زمرة توحيد الخواص

$H_x = \{h \in H \mid hxh^{-1} = x\} = \{h \in H \mid hx = xh\}$ هى **مركز x فى H** (centralizer of x in H)

(راجع مثال ٥٤ فى أمثلة متنوعة على الباب الأول) وسنشير إليه بالرمز $C_H(x)$. وإذا كانت $H = G$ فإننا سنسميه ببساطة **مركز x** (centralizer of x) وسنشير إليه بالرمز $C(x)$. وإذا كانت H تعمل بالترافق على S مجموعة كل الزمر الجزئية لـ G ، عندئذ فإن الزمرة الجزئية فى H المثبتة $K \in S$ وهى بالدقة $\{h \in H \mid hKh^{-1} = K\}$ هي **مطبع K فى H** (normolizer of K in H) ونشير إليها بالرمز $Nor_H(K)$. وإذا كانت $H = G$ سنكتب ببساطة $Nor(K)$ (راجع مثال (١-٦-٦)). وواضح أن كل زمرة جزئية K تكون زمرة جزئية طبيعية فى $Nor(K)$ ، K زمرة جزئية طبيعية فى G إذا كان وفقط إذا كان $Nor(K) = G$.

٥-١-٦ نظرية : إذا كانت الزمرة G تعمل على المجموعة S ، عندئذ فإن العدد الرئيس (The cardinal number) لمسار $x \in S$ هو الدليل $[G : G_x]$.

البرهان : ليكن $g, h \in G$. لأن :

$$gx = hx \Leftrightarrow g^{-1}hx = x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow hG_x = gG_x,$$

وينتج أن الراسم المعطى بـ $gG_x \mapsto gx$ يكون معرفاً جيداً وهو تناظر أحادى من مجموعة المجموعات المشاركة لـ G_x فى G على المسار $\overline{x} = \{gx \mid g \in G\}$. ومن ثم فإن $[G : G_x]$ يساوى العدد الرئيس $\overline{x}$.

٥-١-٧ نتيجة : لتكن G زمرة منتهية ، K زمرة جزئية من G .

(أ) عدد عناصر فصل الترافق لـ $x \in G$ هو $[G : C(x)]$ ، الذى يقسم رتبة (G)

(ب) إذا كانت $\overline{x}_1,\ldots,\overline{x}_n (x_i \in G)$ فصول تكافؤ مختلفة لـــ G ، فإننا نحصل على المعادلة الآتية التى تسمى **معادلة الفصل للزمرة المنتهية** G (The class equation of the finite group G)

$$Ord(G) = \sum_{i=1}^{n} [G : C(x_i)]$$

(جـــ)عدد الزمر الجزئية من G التى تترافق مع K هو$[G:Nor(K)]$ وهو قاسم لرتبة (G)

البرهان : (أ) ، (جــ) تنتجان مباشرة من النظرية (٥-١-٦) ونظرية لاجرانج (١-١٠-٣). ونظراً لأن الترافق هو علاقة تكافؤ على G (نظرية (٥-١-٣)) فإن G تكون الاتحاد المنفصل (The disjoint union) لفصول الترافق $\overline{x}_1,\overline{x}_2,\ldots,\overline{x}_n$ ، وباستخدام (أ) ينتج (ب)

٥-٢ نظريات سيلو The Sylow Theorems

٥-٢-١ نظرية كوشى Cauchy Theorem

لتكن G زمرة إبدالية منتهية ، وليكن p عدداً أولياً قاسماً لرتبة (G). عندئذ فإن G تحتوى على عنصر رتبته p .

البرهان : بالاستقراء الرياضى على رتبة (G) . إذا كانت رتبة (G) هى p فإن النتيجة تنتج مباشرة . إذا لم تكن رتبة (G) هى p فليكن $y \in G$ أى عنصر . والآن نعتبر الحالتين :

الحالة الأولى : يوجد عنصر $y \in G$ بحيث إن p يقسم رتبة (y) ، أى أن $Ord(y) = p\ell, \ell \in \mathbb{N}$. عندئذ فإن: $(y^\ell)^p = y^{p\ell} = e$ (e العنصر المحايد فى G) أى أنه يوجد عنصر $x = y^\ell$ ورتبته هى p .

الحالة الثانية : p ليس قاسماً لرتبة (y) حيث y هو أى عنصر ينتمى إلى G . نكون $\overline{G} = G/[y]$. والآن p قاسم لرتبة (G) ، وليس قاسماً لرتبة (y) ونعلم أن رتبة (y) تقسم رتبة (G). وهذا يستلزم أن :

$$p \,|\, {}^{Ord(G)}\!/_{Ord(y)} = Ord({}^{G}\!/_{[y]}) < Ord(G) \qquad (p|x \text{ أى } p \text{ يقسم } x)$$

ومن فرض الاستقراء الرياضى ينتج أنه يوجد $\bar{z}$ ينتمى إلى $\bar{G}$ بحيث إن $Ord(\bar{z}) = p$
أى أن : $(\bar{z})^p = \bar{e} = e[y]$.

والآن ليكن $Ord(z) = m$ ، أى أن $z^m = e$ وهذا يقتضى أن $(\overline{z^m}) = \bar{e}$ أى أن
$(\bar{z})^m = \bar{e}$ ، ولكن $Ord(\bar{z}) = p$ فهذا يستلزم أن $p|m = Ord(z)$. وهذا تناقض لأنه
من الفرض أن $\forall y \in G \;\; p \nmid Ord(y)$ ($p \nmid x$ تعنى p لا يقسم x)
أى أن الحالة (2) مستحيلة وبهذا ينتهى البرهان .

ملحوظة : الزمرة الجزيئة المتولدة بعنصر رتبته p أيضاً لها الرتبة p ، أى أن G لها زمرة جزئية رتبتها p .

٥-٢-٢ ملحوظة : إذا كان $g \in Z(G)$ (أى أن g عنصر من عناصر مركز الزمرة G)
فإن فصل الترافق لـ g يتكون من g فقط لأن $\forall x \in G \;\; xgx^{-1} = g$. وبالتالى فإنه إذا
كانت G منتهية وكان $x \in Z(G)$ فإنه من (٥-١-٧ (أ)) يكون $[G : C(x)] = 1$ ،
ومن ثم فإنه يمكن كتابة معادلة الفصل فى (٥-١-٧) كالآتى :

$$Ord(G) = Ord(Z(G)) + \sum_{i=1}^{m} \; [G : C(x_i)]$$

حيث $\bar{x}_1, \bar{x}_2, ..., \bar{x}_m (x_i \in G \setminus Z(G))$ فصول ترافق مختلفة لـ G وكل منها يحقق
$[G : C(x_i)] > 1$

٥-٢-٣ نظرية سيلو الأولى Sylow's First Theorem

لتكن G زمرة منتهية بحيث إن $p^m | Ord(G)$ ، $p^{m+1} \nmid Ord(G)$ حيث p عدد أولى ، m عدد صحيح موجب . عندئذ فإن G تحتوى على زمر جزئية من الرتب p ، p^2 ، ... ، p^m

البرهان : النظرية تنتج مباشرة إذا كانت رتبة (G) هى p (أى هى زمرة دائرية لها الرتبة p). سنجرى الاستقراء الرياضى على $Ord(G)$ ، ولنفترض أن النظرية متحققة لجميع الزمر K التى لها رتبة أصغر من $Ord(G)$.

والآن نعتبر $Z(G)$: مركز (G) . توجد لدينا حالتان : $p \nmid Ord(Z(G))$ أو $p \mid Ord(Z(G))$.

فى الحالة $p \mid Ord(Z(G))$: من نظرية كوشى (٥-٢-١) للزمر الإبدالية يوجد $a \in Z(G)$ ، $a \neq e$ ، بحيث إن $a^p = e$. عندئذ فإن $H = [a]$ يكون زمرة جزئية طبيعية من G (لأن $a \in Z(G)$) لها الرتبة p ، ويكون

$$Ord(G/H) = Ord(G)/Ord(H) = Ord(G)/p$$

أى أن $p^{m-1} \mid Ord(G/H)$ ، $p^m \nmid Ord(G/H)$. وبتطبيق فرض الاستقراء ينتج أن G/H لها الزمر الجزئية $\bar{K}_i = K_i/H$ من الرتب p ، p^2 ، ... ، p^{m-1} ، ومن ثم فإن H ، K_1 ، ... ، K_{m-1} تكون زمراً جزئية من G لها الرتب p ، p^2 ، ... ، p^m على الترتيب .

فى الحالة $p \nmid Ord(Z(G))$: سنكتب معادلة الفصل (٥-٢-٢) :

$$Ord(G) = Ord(Z(G)) + \sum_a Ord(G)/Ord(C(a))$$

حيث يجرى الجمع على العناصر a ، بأخذ عنصر واحد من كل فصل ترافق لـ G يتكون من أكثر من عنصر واحد .

ولأن $p \nmid Ord(Z(G))$ ، $p \mid Ord(G)$ ، فإنه يوجد عنصر $a \in G$ بحيث إن $C(a) \neq G$ ، $P \nmid \frac{Ord(G)}{Ord(C(a))}$ وهذا يقتضى أن $p^m \mid Ord(C(a))$. ولأن $C(a) \neq G$ فإنه بتطبيق فرض الاستقراء على $C(a)$ ينتج أن الزمر الجزئية من $C(a)$ ذات الرتب p ، p^2 ، ... ، p^m هى الزمر المنشودة من G .

<u>**٥-٢-٤ نتيجة**</u> : إذا كان $p \mid Ord(G)$ حيث G زمرة منتهية ، p عدد أولى ، فإن G تحتوى على عنصر رتبته p .

وتكون هذه النتيجة تعميماً لنظرية كوشى لزمرة منتهية ليست بالضرورة إبدالية .

٥-٢-٥ تعريف : زمر سيلو Sylow groups : لتكن G زمرة منتهية بحيث إن $p^m | Ord(G)$ ، $p^{m+1} \nmid Ord(G)$ ، حيث p عدد أولى ، m عدد صحيح موجب . عندئذ فإن كل زمرة جزئية من G لها الرتبة p^m تسمى **زمرة سيلو – p الجزئية من G** . (Sylow p – subgroup of G)

٥-٢-٦ مثال : فى $S_3 (= \gamma_3)$ الزمرة الإبدالية على عناصر ثلاثة : تحتوى S_3 على واحدة فقط كزمرة سيلو – 3 – الجزئية هى $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ ، كما تحتوى على ثلاث زمر سيلو – 2 الجزئية هى: $\{e, (1\ 2)\}$ ، $\{e, (1\ 3)\}$ ، $\{e, (2\ 3)\}$ (e هو العنصر المحايد أى الراسم 1_{S_3}) .

٥-٢-٧ تمهيدية : إذا كانت H زمرة من الرتبة p^n وتعمل على مجموعة منتهية S ، وإذا كانت $S_0 := \{x \in S \mid hx = x\ \forall h \in H\}$ ، عندئذ فإن $Card(S) \equiv Card(S_0) (\text{mod}\, p)$
($Card(X)$: = cardinal number of X)

البرهان : المسار $\bar{x}$ يتكون بالضبط من عنصر واحد إذا كان وفقط إذا كان $x \in S_0$. ومن ثم فإن S يمكن أن تكتب فى صورة اتحاد منفصل (disjoint union) $S = S_0 \cup \bar{x}_1 \cup \bar{x}_2 \cup \ldots \cup \bar{x}_n$ ، حيث $Card(x_i) > 1$ لجميع i . وبالتالى فإن : $Card(S) = Card(S_0) + Card(\bar{x}_1) + Card(\bar{x}_2) + \ldots + Card(\bar{x}_n)$. والآن $p \mid Card(\bar{x}_i)$ لجميع i لأن $Card(\bar{x}_i) > 1$ ، $Card(\bar{x}_i) = [H : H_{x_i}] \mid Ord(H) = p^n$. ومن ثم فإن $Card(S) = Card(S_0) (\text{mod}\, p)$.

(تذكر : "$x|y$" تعنى x يقسم y)

٥-٢-٨ تعريف : يقال لزمرة رتبة كل عنصر فيها قوة (= أس) أكبر من أو تساوى الصفر لعدد أولى p إنها **زمرة – p** . (**p – group**) . وإذا كانت H زمرة جزئية من زمرة G ، وكانت H زمرة–p فإنه يقال إن H هى **زمرة جزئية – p من G** . (p – subgroup of G) . وعلى وجه الخصوص فإن $[e]$ هى زمرة جزئية – p من G لجميع الأعداد الأولية p ، لأن $Ord([e]) = 1 = p^0$. (لاحظ أن P زمرة سيلو–p الجزئية من G هى زمرة جزئية – p عظمى من G (أى أن $G \hookleftarrow H \hookleftarrow P$ ، H زمرة – $p \Leftarrow P = H$))

٥-٢-٩ نتيجة : الزمرة المنتهية G تكون زمرة $p-$ إذا كان وفقط إذا كان $Ord(G)$ هو قوة (= أس) لـــ p .

البرهان : إذا كانت G زمرة $p-$ ، وكان q عدداً أولياً قاسماً لرتبة G ، فإن G يحتوى عنصراً له الرتبة q (نظرية كوشى) . نظرا لأن كل عنصر فى G رتبته قوة لـــ p فإن $q=p$. وبالتالـــى فإن رتبة (G) تكون قوة من قوى p . العكس هو نتيجة مباشرة من نظرية لاجرانج (١-١٠-٣) .

٥-٢-١٠ نظرية : إذا كانت G زمرة لها الرتبة $p^n m$ ، حيث p عدد أولى ، $n \geq 1$ ، $\gcd(m,p)=1$ ، وكانت H زمرة جزئية $p-$ من G فإن :

(أ) H زمرة سيلو $p-$ الجزئية من G إذا كان وفقط إذا كان $Ord(H)=p^n$

(ب) كل ترافق لزمرة سيلو $p-$ الجزئية هو زمرة سيلو $p-$ الجزئية

(جـــ) إذا كانت P زمرة سيلو $p-$ الجزئية وحيدة فإن P تكون زمرة جزئية طبيعية من G

البرهان: (أ) تنتج من نظرية لاجرانج (١-١٠-٣) ، النتيجة (٥-٢-٩) ، نظرية سيلو الأولى (٥-٢-٣)

(ب) تنتج من التقرير : [H زمرة جزئية من G $\Leftarrow$ aHa^{-1} زمرة جزئية من G لجميع $a \in G$ وتكون متشاكلة مع H] ، من (أ)

(جـــ) تنتج من (ب) .

ولدينا عكس الجزء (ب) من النظرية السابقة مباشرة (٥-٢-١٠) :

٥-٢-١١ نظرية سيلو الثانية Second Sylow Theorem

إذا كانت H زمرة جزئية $p-$ من زمرة منتهية G، ولتكن P أية زمرة سيلو $p-$ الجزئية من G ، عندئذ فإنه يوجد $x \in G$ بحيث إن $H \longrightarrow xPx^{-1}$ (H زمرة جزئية من xPx^{-1}) وعلى وجه الخصوص فإن أى زمرتين سيلو $p-$ جزئيتين من G تكونان مترافقتين .

البرهان : لتكن S مجموعة المجموعات المشاركة اليسرى من G بالنسبة إلى P ، ولتكن H تعمل على S بالنقل (الأيسر)((left) translation). عندئذ فإنه من التمهيدية (٥-٢-٧)

$$Card(S_0) \equiv Card(S) = [G:P] (\text{mod}\, p)$$

ولكن $p \nmid [G:P]$ (لأن P زمرة جزئية $p-$ عظمى من G ومن نظرية لاجرانج (١-١٠-٣)) ، وبالتالى فإن $Card(S_0) \neq 0$ ، ويوجد $xP \in S_0$.

$$xP \in S_0 \Leftrightarrow hxP = xP \quad \forall h \in H$$

$$\Leftrightarrow x^{-1}hxP = P \ \ \forall h \in H \Leftrightarrow x^{-1}Hx \hookrightarrow P \Leftrightarrow H \hookrightarrow xPx^{-1}$$

وإذا كانت H زمرة سيلو $p-$ الجزئية فإن : $Ord(H) = Ord(P) = Ord(xPx^{-1})$

ومن ثم فإن : $H = xPx^{-1}$

٥-٢-١٢ نظرية سيلو الثالثة Third Sylow Theorem

إذا كانت G زمرة منتهية ، وكان p عدداً أولياً ، عندئذ فإن عدد زمر سيلو $p-$ الجزئية من G يقسم رتبة (G) ، ويكون على الصورة $kp+1$ حيث $k \geq 0$

البرهان : من نظرية سيلو الثانية يكون عدد زمر سيلو $p-$ الجزئية هو عدد الترافقات (conjugates) لأية واحدة منها ، ولتكن P . ولكن هذا العدد هو $[G: Nor(P)]$ وهو قاسم لرتبة (G) من (٥-١-٧). لتكن S مجموعة كل زمر سيلو $p-$ الجزئية من G ، ولتكن P تعمل على S بالترافق . عندئذ فإن $Q \in S_0$ إذا كان وفقط إذا كان $xQx^{-1} = Q$ لجميع $x \in P$. الشرط الأخير يتحقق إذا كان وفقط إذا كان $P \hookrightarrow Nor(Q)$. كلتا P ، Q زمرتا سيلو $p-$ الجزئيتان من G ومن ثم من $Nor(Q)$ ومن ثم فهما تترافقان فى $Nor(Q)$. لكن لأن Q زمرة جزئية طبيعية فى $Nor(Q)$ ، يحدث هذا فقط إذا كان $Q = P$. وبالتالى فإن $S_0 = \{P\}$ ومن التمهيدية (٥-٢-٧) يكون $Card(S) \equiv Card(S_0) = 1 (\bmod p)$. ومن ثم فإن $Card(S) = kp+1$.

٥-٢-١٣ أمثلة محلولة :

مثال١ : برهن على أن $Z(G)$ مركز زمرة $p-$ المنتهية غير التافهة يحتوى على أكثر من عنصر واحد .

البرهان : نعتبر معادلة الفصل لـ G فى (٥-٢-٢) :

$$Ord(G) = Ord(Z(G)) + \sum_{i=1}^{m} [G: C(x_i)]$$

ونظراً لأن كل $[G:C(x_i)]>1$، ويقسم $Ord(G)=p^n$ $(n\geq 1)$ فإن p تقسم كل $[G:C(x_i)]$ ، وتقسم $Ord(G)$ ومن ثم فإن p تقسم $Ord(Z(G))$. ونظراً لأن $Ord(Z(G))\geq 1$ فإن $Z(G)$ يحتوى على أزيد من عنصر .

<u>مثال ٢</u> : إذا كانت H زمرة جزئية $p-$ من زمرة منتهية G ، عندئذ فإن

$$[Nor(H):H]\equiv[G:H](\bmod p)$$

<u>البرهان</u> : لتكن S هى مجموعة المجموعات المشاركة اليسرى من G بالنسبة إلى H ، ولتكن H تعمل على S بالنقل (الأيسر) . عندئذ فإن $Card(S)=[G:H]$. كذلك فإن :

$$xH\in S_0 \Leftrightarrow hxH=xH \quad \forall h\in H$$

$$\Leftrightarrow x^{-1}hxH=H \ \ \forall h\in H \ \ \Leftrightarrow x^{-1}hx\in H \quad \forall h\in H$$

$$\Leftrightarrow x^{-1}Hx=H \quad \Leftrightarrow xHx^{-1}=H$$

$$\Leftrightarrow x\in Nor(H)$$

ومن ثم فإن $Card(S_0)$ هو عدد المجموعات المشاركة xH حيث $x\in Nor(H)$ ، أى أن $Card(S_0)=[Nor(H):H]$. ومن التمهيدية (٥-٢-٧) ينتج أن :

$$[Nor(H):H]=Card(S_0)\equiv Card(S)(\bmod p)=[G:H](\bmod p)$$

<u>مثال ٣</u> : إذا كانت H زمرة جزئية $p-$ من زمرة منتهية G بحيث إن p تقسم $[G:H]$ ، فإن $Nor(H)\neq H$

<u>البرهان</u> : لدينا $0\equiv[G:H]\equiv[Nor(H):H](\bmod p)$. من حيث إن p تقسم $[G:H]$ ، ولأن $[Nor(H):H]\geq 1$ فإن $[Nor(H):H]>1$. وبالتالى فإن : $Nor(H)\neq H$

<u>مثال ٤</u> : حدد إذا ما كانت التقريرات الآتية صحيحة أو خاطئة :

(أ) كل زمرتى سيلو $p-$ الجزئيتين من زمرة منتهية تكونان مترافقتين (conjugate)

(ب) كل زمرة ذات الرتبة 15 تحتوى على زمرة سيلو $-$ 5 الجزئية الوحيدة

(جـ) كل زمرة سيلو $p-$ الجزئية من زمرة منتهية تكون رتبتها قوة (أس) لـ p

(د) كل زمرة إبدالية منتهية G تحتوى على زمرة سيلو – p الجزئية الوحيدة لكل عدد أولى p يقسم رتبة الزمرة G

(هـ) كل زمرة جزئية – p من زمرة منتهية تكون زمرة سيلو – p الجزئية

(و) فصل الترافق لكل عنصر فى كل زمرة يكون زمرة جزئية من الزمرة .

(ز) عناصر المركز فى زمرة منتهية تكون مترافقة (conjugate)

(ح) مبدأ فصل الترافق معرف فقط على الزمر المنتهية .

<u>الحـل</u> : (أ) صحيح (ب) صحيح (جـ) صحيح (د) صحيح

(هـ) خطأ (و) خطأ (ز) خطأ (ح) خطأ

<u>مثال ٥</u> : اوجد فصل الترافق لأى عنصر فى زمرة إبدالية G .

<u>الحـل</u> : فى أية زمرة إبدالية :

$$xax^{-1} = xx^{-1}a = ea = a$$

إذن فصل الترافق لعنصر هو المجموعة المكونة من العنصر فقط :

$$\{xax^{-1} \mid x \in G\} = \{a\}$$

<u>مثال ٦</u> : حقق نظرية سيلو الثالثة حيث $p = 2$ ، بالنسبة إلى S_3 .

<u>الحـل</u> : رتبة S_3 هى6 . زمر سيلو – 2 الجزئية من S_3 هى :

$\{e, (1\ 2)\}$ ، $\{e, (1\ 3)\}$ ، $\{e, (2\ 3)\}$ حيث e هو العنصر المحايد .

عدد هذه الزمر 3 ، ويكون على الصورة 1 + 2 ، أى $1 + 2k$ حيث $k = 1$ ، وكذلك 3 يقسم 6 (هى رتبة S_3) .

<u>مثال ٧</u> : اوجد رتبة زمرة سيلو – 3 الجزئية من زمرة رتبتها 12 .

<u>الحـل</u> : $12 = 4.3^1$. وبالتالى تكون رتبة زمرة سيلو – 3 الجزئية هى 3 .

<u>مثال ٨</u> : اوجد رتبة زمرة سيلو – 3 الجزئية من زمرة رتبتها 54

<u>الحل</u> : $54 = 2.3^3$ وبالتالى تكون رتبة زمرة سيلو– 3 الجزئية هى 3^3 أى 27 .

<u>مثال ٩</u> : اوجد العدد المحتمل لزمر سيلو – 2 الجزئية من زمرة رتبتها 24

الحـــل : عدد الزمر قاسم لرتبة الزمرة 24 ، وكذلك يكون على الصورة $1+2k$ ، $k \in \mathbb{N}$ وبهذا يكون العدد إما 1 بأخذ $k=0$ أو 3 بأخذ $k=1$.

مثال ١٠ : اوجد العدد المحتمل لزمر سيلو – 3 الجزئية ولزمر سيلو – 5 الجزئية من زمرة رتبتها 255 .

الحـــل:(17) (5) (3) = 255 . العدد المحتمل لزمر سيلو– 3 الجزئية يكون قاسماً لــ255 وكذلك يكون على الصورة $1+3k$ حيث $k \in \mathbb{N}$. ومن ثم فإن العدد يكون 1 بأخذ $k=0$ أو 85 بأخذ $k=28$.

العدد المحتمل لزمر سيلو – 5 الجزئية يكون كذلك قاسماً لــ 255 ويكون على الصورة $1+5k$ حيث $k \in \mathbb{N}$. وبالتالى فإن العدد يكون 1 بأخذ $k=0$ أو 51 بأخذ $k=10$.

مثال ١١ : ما أكبر عدد محتمل من فصول الترافق فى زمرة رتبتها 215 ؟

الحـــل : أكبر عدد محتمل هو 215 لأن الزمرة ربما تكون إبدالية !

من مثال ٥ يكون كل فصل ترافق لعنصر يتكون من العنصر نفسه فقط .

مثال ١٢ : إذا كان $Ord(G)=p^r m$ حيث G زمرة ، $r \geq 1$ ، $p \nmid m$ ، وكانت P زمرة سيلو– p الجزئية من G ، وكانت H زمرة – p بحيث إن $P \subset H \subset G$ فبرهن على أن $H=P$

البرهان : من حيث إن H زمرة – p فإن $Ord(H)=p^t, t \geq 0$ ، ومن نظرية لاجرانج (١–١٠–٣) ينتج أن $p^t \mid p^r m$. ومن حيث إن $p \nmid m$ ينتج أن $p^t \mid p^r$ وبالتالى يكون $t \leq r$. ولكن $P \subset H$ ، $Ord(P)=p^r$ (لأن P زمرة سيلو – p الجزئية من G) فينتج أن $p^r \mid p^t$ أى أن $r \leq t$. ومن ثم فإن $r=t$ ويكون $Ord(P)=Ord(H)$ ومن ثم فإن $P=H$.

مثال ١٣ : إذا كانت G زمرة رتبتها p^2 ، حيث p عدد أولى ، فبرهن على أن G إبدالية.

البرهان : ليكن $Z(G)$ هو مركز G . واضح أن G زمرة – p المنتهية غير التافهة (رتبة أى عنصر فى زمرة يكون قاسماً لرتبة الزمرة من نظرية لاجرانج (١–١٠–٣)) . ومن

مثال ١ فى (٥-٢-١٣) يكون $Z(G)$ محتوياً على أكثر من عنصر واحد . والآن إذا كان $Z(G) = G$ تكون G زمرة إبدالية . أما إذا كان $Z(G) \neq G$ فإن $Ord(Z(G)) = p$ (لأن $Z(G)$ زمرة جزئية (طبيعية) من G وحسب نظرية لاجرانج) وبالتالى يكون $Ord(G/Z(G)) = p$ ،

ومن ثم تكون $G/Z(G)$ زمرة دائرية (١-١١-٧) (٢) ومن مثال ٥٠ من أمثلة متنوعة على الباب الأول ينتج أن G إبدالية .

<u>مثال ١٤</u> : إذا كانت G زمرة غير إبدالية ورتبتها p^3 ، حيث p عدد أولى ، فبرهن على أن $Ord(Z(G)) = p$.

<u>البرهان</u> : G كما سبق فى مثال ١٣ السابق مباشرة زمرة – p المنتهية غير التافهة فمن مثال ١ فى (٥-٢-١٣) يكون $Z(G)$ محتوياً على أزيد من عنصر واحد. كذلك فإن $Z(G) \neq G$ لأن G غير إبدالية . والآن إذا كان $Ord(Z(G)) = p^2$ فإنه ينتج من نظرية لاجرانج (١-١٠-٣) أن $Ord(G/Z(G)) = p$ ومن (١-١١-٧) (٢) ينتج أن G دائرية وبالتالى تكون إبدالية . وهذا تناقض. إذن $Ord(Z(G)) = p$

<u>مثال ١٥</u> : برهن على أن أية زمرة رتبتها 15 لايمكن أن تكون بسيطة (simple) (بسيطة أى لاتحتوى على زمرة جزئية طبيعية غير تافهة أى فعلية)

البرهان : لتكن G زمرة رتبتها 15 . نحن ندعى أن G تحتوى على زمرة جزئية طبيعية من الرتبة 5 (رتبة الزمرة الجزئية قاسم لرتبة الزمرة من نظرية لاجرانج). من نظرية سيلو الأولى (٥-٢-٣) G تحتوى على الأقل على زمرة جزئية من رتبة 5 وعدد هذه الزمر الجزئية يطابق 1 مقياس 5

(congruent to 1 modulo 5) (نظرية سيلو الثالثة) .

ونظراً لأن1 ، 6 ، 11 هى فقط الأعداد التى تقل عن 15 وتكون مطابقة لـــ 1 مقياس 5 ، ونظراً لأن 1 فقط من بين هذه الأعداد الثلاثة الذى يكون قاسماً لرتبة G وهى 15 ، فإننا نجزم بأن G لها بالضبط زمرة جزئية واحدة من الرتبة 5 . ولكن لكل $a \in G$ يرسم

الأوتومورفيزم الداخلى φ_a (انظر (١-٣-٧)) عناصر G كالآتى : $\varphi_a(x)=axa^{-1}$ ، $\forall x\in G$ ، وعلى وجه الخصوص يرسم H على (onto) الزمرة الجزئية aHa^{-1} وتكون رتبتها 5. ولأن G تحتوى على زمرة جزئية وحيدة ذات الرتبة 5 فإن $aHa^{-1}=H$ لجميع $a\in G$. أى أن H زمرة جزئية طبيعية غير تافهة فى G . ومن ثم فإن G ليست بسيطة .

مثال ١٦: برهن على أن أية زمرة غير دائرية G من الرتبة 21 تحتوى على 14 عنصراً من الرتبة 3 .

البرهان : $3\times 7=21$. من نظرية سيلو الأولى تحتوى G على زمرة جزئية واحدة على الأقل من الرتبة 3 ، زمرة جزئية واحدة على الأقل من الرتبة 7 . وعدد الزمر الجزئية من الرتبة 3 يحقق $3k+1$ وهو قاسم لرتبة G (نظرية سيلو الثالثة) . وبالتالى فإن عدد الزمر الجزئية من الرتبة 3 يكون 7. وواضح أن الزمر الجزئية دائرية (١-١١-٧) كذلك من (١-١١-١١) كل زمرة تحتوى على مولدين أى أن G تحتوى على 14 عنصراً من الرتبة 3 .

مثال ١٧ : لتكن G زمرة رتبتها 60 . إذا كانت زمرة سيلو – 3 الجزئية طبيعية فبرهن على أن زمرة سيلو – 5 الجزئية طبيعية كذلك .

البرهان : لتكن M زمرة سيلو – 3 الجزئية ، ولتكن G محتوية على زمر سيلو – 5 الجزئية غير الطبيعية وهى N_1 ، ... (لماذا أكثر من واحدة ؟) . عدد هذه الزمر يقسم 60 (رتبة G) وكذلك يحقق $5k+1$ ، ولأنه توجد أكثر من زمرة سيلو– 5 الجزئية غير الطبيعية فيكون $k=1$ وعدد هذه الزمر 6. أى لدينا N_1 ، N_2 ، ... ، N_6 . هذه الزمر الجزئية تحتوى على 6×4 أى 24 عنصراً من الرتبة 5 (١-١١-١١) . لاحظ كذلك أن MN_1 ، MN_2 ، ... ، MN_6 كلها زمر جزئية من G ((١-٨-٢) النظرية الأولى للأيزومورفيزم) ورتبتها جميعا 15 وبهذا تكون دائرية (لماذا ؟) ومن ثم فإن كل واحدة منها لها 8 مولدات (١-١١-١١) أى أنه يوجد كذلك $8\times 6=48$ عنصراً من الرتبة 15. أى لدينا 72 عنصراً من الرتبة 5 ، الرتبة 15 بينما الزمرة من الرتبة 60 . تناقض .

مثال ١٨ : إذا كان p عدداً أولياً فإن أية زمرة من الرتبة $2p$ تحتوى على زمرة جزئية طبيعية من الرتبة p .

البرهان: وجود هذه الزمرة الجزئية مضمون من نظرية سيلو الأولى . ودليل هذه الزمرة الجزئية = 2 فينتج من مثال ٣٩ من أمثلة على الباب الأول المطلوب مباشرة .

مثال ١٩ : برهن على أنه إذا كانت G زمرة لها الرتبة pq حيث p ، q عددان أوليان ، $p < q$ ، p لاتقسم $q - 1$ ، فإن G تكون دائرية . وعلى وجه الخصوص تكون G متشاكلة مع $\mathbb{Z}_{pq}$.

البرهان : لتكن H زمرة سيلو $- p$ الجزئية من G ، K زمرة سيلو $- q$ الجزئية من G .

من نظرية سيلو الثالثة يكون عدد زمر سيلو$- p$ الجزئية من G ، وليكن n_p على الشكل $1 + kp$ ، ويقسم pq . ومن ثم فإن $1+kp=1$ أو $1+kp=p$ أو $1+kp=q$ أو $1+kp=pq$. من هذا ولأن $p \nmid q-1$ ينتج أن $k=0$ ، وبالتالى فإن H هى زمرة سيلو $- p$ الجزئية الوحيدة فى G .

وبالمثل فإن K هى زمرة سيلو $- q$ الوحيدة فى G . ومن ثم فإن H ، K تكونان زمرتين جزئيتين طبيعيتين من G (انظر مثال ٢٣) والآن ليكن $H=[x]$ ، $K=[y]$ (لاحظ أن H ، K دائريتان) وسنبرهن على أن G دائرية . ويكفى لهذا أن نبرهن على أن x ، y يتبادلان (commute)، وعندئذ فإن $Ord(xy)=Ord(x)Ord(y)=pq$ أى أن xy يولد G أى أن G دائرية . والآن لاحظ أنه لأن H ، K طبيعيتان فإن :

$$x^{-1}y^{-1}xy=(x^{-1}y^{-1}x)y\in Ky=K$$

$$x^{-1}y^{-1}xy=x^{-1}(y^{-1}xy)\in x^{-1}H=H$$

وهكذا فإن $x^{-1}y^{-1}xy\in K\cap H=\{e\}$ ، ومن ثم فإن $xy=yx$.

نهاية البرهان .

مثال ٢٠ : إذا كانت هناك زمرة رتبتها p^n ، حيث p عدد أولى ، وكانت تحتوى على زمرة جزئية وحيدة لكل رتبة p ، p^2 ، ... ، p^{n-1} فبرهن على أن الزمرة دائرية .

البرهان : لتكن G الزمرة التى رتبتها p^n ، H زمرة جزئية منها رتبتها p^{n-1} . من نظرية سيلو الأولى تحتوى H على زمر جزئية من الرتب p ، p^2 ، ... ، p^{n-2} . ونظراً لأن كل هذه الزمر الجزئية هى زمر جزئية فى G كذلك ، فإنه ينتج أن جميع الزمر الجزئية الفعلية (أى غير التافهة) فى G تكون محتواة فى H . والآن إذا كان $a \notin H$ ، $a \in G$ ، فإن رتبة a يجب أن تكون p^n ، وإلا ولد a زمرة جزئية K رتبتها أقل من p^n . وهذا يعنى أن $a \in H$ ، نظراً لأن $a \in K \subset H$. وهكذا فإن رتبة a هى p^n ومن ثم فإن G تكون زمرة دائرية متولدة بـــ a .

مثال ٢١ : إذا كانت H زمرة جزئية طبيعية من زمرة منتهية G رتبتها $p^m q$ ، p عدد أولى ، $(p,q) = 1$، وكان دليل H فى G ليس بينه وبين p قواسم مشتركة عدا الواحد ، عندئذ فإن H تحتوى على كل زمرة سيلو – p الجزئية من G .

البرهان : لدينا $Ord(G) = p^m q$ حيث $(p,q) = 1$ (= القاسم المشترك الأعظم بين p ، q هو الواحد). ونظراً لأن $[G:H] = \dfrac{Ord(G)}{Ord(H)}$ ، وليس بينه وبين p قواسم مشتركة فإن $Ord(H) = p^m q_1$ حيث $(p,q_1) = 1$. من نظرية سيلو الأولى تحتوى H على زمرة سيلو– p الجزئية K حيث $Ord(K)= p^m$، K تكون أيضاً زمرة سيلو – p الجزئية من G. ولتكن K_1 زمرة سيلو – p الجزئية الأخرى من G . عندئذ فإنه من نظرية سيلو الثانية يكون هناك $x \in G$ بحيث إن :

$$K_1 = xKx^{-1} \subset xH^{-1}x \subset H \qquad (\text{لأن } H \triangleleft G)$$

ومن ثم فإن جميع زمر سيلو – p الجزئية من G تكون محتواة فى H .

مثال ٢٢ : ليكن d قاسماً لرتبة زمرة إبدالية منتهية G هى n . عندئذ فإن G تحتوى على زمرة جزئية لها الرتبة d .

البرهان : إذا كان $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ ، فإن

$$G = \mathbb{Z}_{p_1^{e_1}} \otimes \mathbb{Z}_{p_2^{e_2}} \otimes \dots \otimes \mathbb{Z}_{p_r^{e_r}} \qquad (٤-١-١)$$

وليكن $d = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$. من نظرية سيلو الأولى تحتوى $\mathbb{Z}_{p_i^{e_i}}$ على زمرة جزئية $\mathbb{Z}_{p_i^{f_i}}$ ، وعندئذ فإن :

$$H = \mathbb{Z}_{p_1^{f_1}} \otimes \mathbb{Z}_{p_2^{f_2}} \otimes \dots \otimes \mathbb{Z}_{p_r^{f_r}}$$

وهى زمرة جزئية رتبتها d . (قارن مع نظرية كوشى (٥-٢-١))

مثال ٢٣ : برهن على أن زمرة سيلو $p -$ الجزئية من زمرة منتهية G تكون وحيدة إذا كانت وفقط إذا كانت طبيعية .

البرهان : لتكن H زمرة سيلو $p -$ الجزئية طبيعية فى الزمرة المنتهية G . ولتكن K زمرة سيلو $p -$ الجزئية الأخرى فى G . من نظرية سيلو الثانية يكون H ، K مترافقتين، أى أنه يوجد $x \in G$ بحيث إن : $K = xHx^{-1}$. ولكن H طبيعية فى G يستلزم أنه لكل $x \in G$: $H = xHx^{-1}$. وينتج مباشرة أن $H = K$.

والآن لتكن H وحيدة والمطلوب إثبات أنها طبيعية . من حيث إن لكل $x \in G$:

$Ord(xHx^{-1}) = Ord(H)$ ، ينتج أن xHx^{-1} زمرة سيلو $p -$ الجزئية من G ، ولأن H زمرة سيلو $p -$ الجزئية الوحيدة فينتج أن $\forall x \in G \ : \ xHx^{-1} = H$ أى أن H طبيعية . (انظر مثالى ١٧ ، ١٩ السابقين)

مثال ٢٤:برهن على أن أى زمرة من الرتبة105تحتوى على زمرة جزئية من الرتبة 35.

البرهان : من نظرية سيلو الثالثة عدد زمر سيلو $- 7$ الجزئية من G يقسم 105 ، ويكون على الصورة $1 + 7k, k \geq 0$ ، وبالتالى فهو إما أن يكون 1 أو يكون 15 . كذلك يكون عدد زمر سيلو $- 5$ الجزئية من G يقسم 105 ويكون على الصورة $1 + 5k, k \geq 0$ ، وبالتالى فإنه يكون 1 أو 21 . وبحساب عدد العناصر يتضح أنه لابد أن يكون أحد عددى زمرتى سيلو 5 ، 7 السابقتين هو 1 ، أو أن يكون كلا العددين هو 1 . ومن مثال ٢٣ السابق مباشرة نعلم أن زمرة سيلو $p -$ الجزئية الوحيدة من زمرة منتهية تكون طبيعية . أى أن احدى الزمرتين على الأقل طبيعية . ومن برهان النظرية الأولى للأيزومورفيزم

(١-٨-٢) نعلم أنه إذا كانت U زمرة جزئية من زمرة G ، وكانت N زمرة جزئية طبيعية من G فإن $UN := \{un \mid u \in U, n \in N\}$ تكون زمرة جزئية من G . وبالتالى فإنه يكون لدينا زمرة جزئية من الزمرة التى رتبتها 105 ، وتكون رتبة هذه الزمرة الجزئية هى $35 = (5)(7)$.

مثال ٢٥ : لتكن H زمرة – p الجزئية من G . عندئذ فإن $g^{-1}Hg, g \in G$ تكون كذلك زمرة – p الجزئية من G .

البرهان : ليكن $Ord(G) = p^r m, r \geq 0, p \nmid m$ ($p \nmid m$ أى أن p ليس قاسماً لـــ m).

عندئذ فإن $Ord(H) = p^r$. لكن $Ord(g^{-1}Hg) = Ord(H)$ (لماذا ؟) ومن ثم فإنه إذا كانت $g^{-1}Hg$ زمرة جزئية من G فإنها تكون كذلك زمرة – p الجزئية من G .

$g^{-1}Hg$ زمرة جزئية من G لأنها أولاً غير خالية إذ تحتوى على الأقل على e (العنصر المحايد فى G)،

ثانيا : إذا كان $g^{-1}h_1g, g^{-1}h_2g \in g^{-1}Hg$ فإن :

$g^{-1}h_1g(g^{-1}h_2g)^{-1} = g^{-1}h_1gg^{-1}h_2^{-1}g = g^{-1}h_1h_2^{-1}g \in g^{-1}Hg$. ومن (١-٤-٢) ينتج المطلوب مباشرة .

تمارين

(١) اوجد جميع زمر سيلو – 3 الجزئية من S_4 واثبت أنها جميعاً مترافقة (conjugate) (لاحظ أنها جميعا فى A_4 ، وعددها يحقق 1 مقياس 3)

(٢) اعتبر الزمرة الثمانية (مثال٤٥ من أمثلة متنوعة على الباب الأول) (هذه فى الواقع هى D_4 . انظر مثال ٤٨ من أمثلة متنوعة على الباب الأول).

(أ) اوجد "تحليل" D_4 إلى فصول ترافق .

(ب) اكتب معادلة الفصل لـــ D_4 .

(٣) اوجد زمرتى سيلو – 2 الجزئيتين من S_4 وبرهن على أنهما مترافقتان

(٤) إذا كانت H مجموعة جزئية من زمرة منتهية G ، وكانت $g \in G$ فبرهن على أن عدد عناصر H = عدد عناصر $g^{-1}Hg$ حيث $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$

(٥) اوجد فصول الترافق فى S_3 ، ومن ثم اكتب معادلة الفصل

(٦) فى S_3 هناك ثلاث زمر سيلو – 2 الجزئية . حقق أن أى اثنتين منها يمكن الحصول عليهما من الثالثة بالترافق

(٧) لتكن G زمرة ، X مجموعة غير خالية

(أ) إذا كانت τ عملية من G على X (أى أن G تعمل على X – انظر التعريف (٥–١–(١)) فإنه لكل $a \in G$ يكون الراسم

$$\begin{aligned} \tau_a : X &\to X \\ x &\mapsto \tau(a,x) \end{aligned}$$

تناظراً أحادياً ، ويكون الراسم :

$$\begin{aligned} G &\to \gamma(G) \\ a &\mapsto \tau_a \end{aligned}$$

(انظر مثال ٣ من أمثلة (١–٢–٥))

هومومورفيزم زمر .

(ب) إذا كان $\varphi : G \to \gamma(X)$ هومومورفيزم زمر فإن الراسم :

$$G \times X \to X$$
$$(a,x) \mapsto \varphi(a)(x)$$

يكون عملية من G على X .

(٨) اعرض زمرة سيلو – 2 جزئية من S_4 وصف تشاكلا (أيزومورفيزما) منها مع D_4

(٩) برهن على أن الترافق علاقة تكافؤ على مجموعة

(١٠) لتكن G زمرة رتبتها 168 . إذا كانت G تحتوى على أكثر من زمرة سيلو – 7 الجزئية فكم بالضبط تحتوى من تلك الزمر ؟

(١١) برهن على أن أية زمرة رتبتها 56 تحتوى على زمرة جزئية طبيعية غير تافهة

(١٢) كم عدد زمر سيلو – 5 الجزئية من S_5 ؟ اذكر اثنتين منها

(١٣) إذا كانت G زمرة غير دائرية رتبتها 21 فكم عدد زمر سيلو – 3 الجزئية من G ؟

(١٤) برهن على أن جميع زمر سيلو – p الجزئية من زمرة منتهية تكون متشاكلة (أيزومورفية)

(١٥) برهن على أنه إذا كان p عدداً أولياً ، وكان كل عنصر فى زمرة منتهية ذا رتبة هى قوة (أس) من قوى p فإن رتبة G تكون كذلك قوة من قوى p

(١٦) لتكن H زمرة جزئية طبيعية من زمرة G . برهن على أن H هى اتحاد فصول الترافق لعناصر H. هل يتحقق هذا كذلك إذا لم تكن H طبيعية فى G ؟

(١٧) كم عدد زمر سيلو – 3 الجزئية من S_5 ؟ اذكر خمساً منها

(١٨) اوجد جميع زمر سيلو – 3 الجزئية من S_4 وبرهن على أنها جميعاً مترافقة

(١٩)لتكن G زمرة على مجموعة X. وليكن $a \in X$. تذكر أن <u>مثبت</u>(a) (stabilizer) هو $stab(a) := \{\alpha \in G \mid \alpha(a) = a\}$. برهن على أن $stab(a)$ زمرة جزئية من G .

1 Group Theory نظرية الزمر

القسم

الباب 6

المتسلسلات الطبيعية ومتسلسلات التركيب والزمر القابلة للحل

Normal Series, Composition Series and Solvable Groups

٦-١ المتسلسلات الطبيعية ومتسلسلات التركيب

٦-١-١ تعريف : **المتسلسلة الطبيعية** لزمرة G هى متوالية منتهية $(G_0, G_1, ..., G_r)$ من الزمر بحيث يكون $\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd ... \lhd G_r = G$ ، حيث e هو عنصر G المحايد ، $H \lhd G$ تعنى H زمرة جزئية طبيعية من G . وواضح أن كل زمرة لها متسلسلة طبيعية $(\{e\}, G)$

وواضح كذلك أنه إذا كانت $(G_0, G_1, ..., G_r)$ متسلسلة طبيعية فإن هذا يعنى وجود سلسلة (chain) متصاعدة (ascending) من الزمر الجزئية :

$\{e\} = G_0 \subset G_1 \subset G_2 \subset ... \subset G_r = G$

٦-١-٢ تعريف : يقال إن متسلسلتين طبيعيتين لزمرة G $(G_0, G_1, ..., G_r)$ ، $(G'_0, G'_1, ..., G'_s)$ **متكافئتان** (equivalent) وسنكتب $(G_0, G_1, ..., G_r) \sim (G'_0, G'_1, ..., G'_s)$ إذا كان $s = r$ ، يوجد $\sigma_i \in S_r$ (تبديلة من الزمرة المتماثلة من الرتبة r) بحيث يكون :

$$G_i / G_{i-1} \cong G'_{\sigma(i)} / G'_{\sigma(i)-1} \quad , 1 \le i \le r$$

٦-١-٣ ملحوظة : "$\sim$" هى علاقة تكافؤ على مجموعة المتسلسلات الطبيعية لزمرة G.

٦-١-٤ تعريف : يقال **لزمرة جزئية طبيعية** H فى زمرة G إنها **عظمى** (maximal) إذا كانت $H \neq G$ ، ولا يوجد زمرة جزئية طبيعية K بحيث يكون

$$H \underset{\neq}{\subset} K \underset{\neq}{\subset} G$$

٦-١-٥ أمثلة : (١) فى الزمرة $\mathbb{Z}$: لكل عدد أولى $p \in \mathbb{P}$: $p\mathbb{Z}$ زمرة جزئية طبيعية عظمى ، ولا توجد فى $\mathbb{Z}$ زمر جزئية طبيعية عظمى أخرى .

(٢) فى $S_3 (= \gamma_3)$: الزمرة الجزئية الطبيعية غير التافهة الوحيدة هى $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ (حيث e العنصر المحايد) ، وهى عظمى (انظر مثال ٩ من أمثلة متنوعة على المفاهيم الأساسية)

(٣) الزمرة A_n ، زمرة التبديلات الزوجية زمرة جزئية طبيعية وهى عظمى .

٦-١-٦ تعريف : يقال لزمرة إنها **بسيطة** (simple) إذا لم تحتو من الزمر الطبيعية إلا التافهة .

٦-١-٧ تمهيدية : إذا كانت H زمرة جزئية طبيعية فعلية (مضبوطة) من G (أى H زمرة جزئية من G ولاتساوى G) فإن G/H تكون بسيطة إذا كانت وفقط إذا كانت H زمرة جزئية طبيعية عظمى من G.

البرهان : هذا ينتج مباشرة من تعريف الزمرة الجزئية الطبيعية العظمى ومن ملاحظة أنه إذا كانت G/K الزمرة العاملة لـــ G فإن أية زمرة جزئية من G/K سيكون لها الشكل H/K ، حيث H زمرة جزئية من G تحتوى على K ؛ و H/K زمرة جزئية طبيعية من G/K إذا كانت وفقط إذا كانت H زمرة جزئية طبيعية من G .

٦-١-٨ تمهيدية : إذا كانت H ، K زمرتين جزئيتين طبيعيتين عظميين مختلفتين من زمرة G ، فإن $H \cap K$ زمرة جزئية طبيعية عظمى من H ومن K .

البرهان : من (١-٨-٢) النظرية الأولى للأيزومورفيزم $HK/K \cong H/H \cap K$ والآن من مثال ٤٢ (أمثلة متنوعة على الباب الأول) HK زمرة جزئية طبيعية من G . والآن $K \subset HK$, K زمرة جزئية عظمى من G فينتج أن $HK = K$ أو $HK = G$. ليكن $HK = K$. هذا يستلزم أن $H \subset K$. ولكن H زمرة جزئية عظمى من G فينتج أن $H = K$ أو أن $K = G$. كلاهما مرفوض لأنه يتناقض مع الفرض . ومن ثم فإن $HK = G$. وبالتالى فإن :

$$H/H \cap K \cong G/K$$

ومن حيث إن K زمرة جزئية طبيعية عظمى من G فإن $H \cap K$ زمرة جزئية طبيعية عظمى من H. وبالمثل فإن $H \cap K$ زمرة جزئية طبيعية عظمى من K .

٦-١-٩ تعريف : **متسلسلة التركيب** (composition series) هى متسلسلة طبيعية $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{r-1} \subset G_r = G$ فيها كل G_i هى زمرة جزئية طبيعية عظمى من G_{i+1} ، أى أن G_{i+1}/G_i زمرات بسيطة .

وتسمى زمر القسمة G_{i+1}/G_i **عوامل التركيب** (composition factors) .

٦-١-١٠ أمثلة : (١) $\{e\} \subset \{e,(1\ 2\ 3),(1\ 3\ 2)\} \subset S_3$ متسلسلة تركيب لـــ S_3 .

$$\{e\} \subset \{e,(1\ 2)(3\ 4)\} \subset \{e,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\} \subset A_4 \subset S_4$$

متسلسلة نركيب لـــ S_4 .

(٢) $$\{e\} \subset \{e,\alpha^2\} \subset \{e,\alpha,\alpha^2,\alpha^3\} \subset G$$

متسلسلة تركيب للزمرة الثمانية (انظر مثال ٤٥ من أمثلة متنوعة على الباب الأول)

(٣) $$\{\bar{0}\} \subset \{\bar{0},\bar{9}\} \subset \{\bar{0},\bar{3},\bar{6},\bar{9},\overline{12},\overline{15}\} \subset \{\bar{0},\bar{1},\bar{2},\ldots,\overline{17}\} = \mathbb{Z}/18\mathbb{Z}$$

متسلسلة تركيب لـــ $\mathbb{Z}/18\mathbb{Z}$

٦-١-١١ نظرية : أى زمرة منتهية G لها متسلسلة تركيب

البرهان : إذا كانت $G = \{e\}$ فالادعاء تافه .

نفترض أن الادعاء صحيح للزمر ذات الرتبة الأقل من $Ord(G)$. إذا كانت G بسيطة فالادعاء تافه. لتكن H زمرة جزئية طبيعية غير تافهة فى G . من فرض الاستقراء الرياضى سيكون لـــ H ، G/H متسلسلتا تركيب ، هما :

$$\{e\} \subset H_1 \subset H_2 \subset \ldots \subset H_n = H,$$

$$H/H =: G_0/H \subset G_1/H \subset G_2/H \subset \ldots \subset G_m/H = G/H$$

ونحصل منهما على

$$\{e\} \subset H_1 \subset H_2 \subset \ldots \subset H_{n-1} \subset H = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_m = G$$

وهذه متسلسلة تركيب لأن :

$$G_{i+1}/G_i \cong \left(G_{i+1}/H\right)\Big/\left(G_i/H\right), 0 \le i \le m-1$$

٦-١-١٢ نظرية جوردان – هولدر Jordan – Holder Theorem

إذا كانت G زمرة منتهية ، فإن أى متسلسلتى تركيب تكونان متكافئتين .

البرهان : بالاستقراء الرياضى على رتبة G . ليكن

$$\{e\} = A_0 \subset A_1 \subset \ldots \subset A_{r-1} \subset A_r = G,$$

$$\{e\} = B_0 \subset B_1 \subset \ldots \subset B_{s-1} \subset B_s = G$$

متسلسلتى تركيب لـــ G . إذا كان $A_{r-1} = B_{s-1}$ فإن الادعاء ينتج مباشرة من فرض الاستقراء الرياضى. ليكن $A_{r-1} \neq B_{s-1}$. وليكن

$$\{e\} = C_0 \subset C_1 \subset C_2 \subset \ldots \subset A_{r-1} \cap B_{s-1}$$

متسلسلة تركيب لـــ $A_{r-1} \cap B_{s-1}$

لدينا من (٦-١-٨) $A_{r-1} \cap B_{s-1}$ زمرة جزئية طبيعية عظمى من A_{r-1} ، أيضاً من B_{s-1} ، ومن ثم فإن السلاسل (chains) الآتية تكون متسلسلات تركيب لـــ G :

$$S_1 : \{e\} = A_0 \subset A_1 \subset \ldots \subset A_{r-1} \subset A_r = G$$

$$S_2 : \{e\} = C_0 \subset C_1 \subset \ldots \subset A_{r-1} \cap B_{s-1} \subset A_{r-1} \subset A_r = G$$

$$S_3 : \{e\} = C_0 \subset C_1 \subset \ldots \subset A_{r-1} \cap B_{s-1} \subset B_{s-1} \subset B_s = G$$

$$S_4 : \{e\} = B_0 \subset B_1 \subset \ldots \subset B_{s-1} \subset B_s = G$$

من فرض الاستقراء الرياضى A_{r-1} ، B_{s-1} لهما متسلسلتا تركيب متكافئتان . وإذا حذفنا الحدين الأخيرين فى S_1 ، S_2 فإن السلسلتين الناتجتين تكونان متسلسلتى تركيب لـــ A_{r-1} ، ومن ثم فمن فرض الاستقراء الرياضى تكون السلسلتان متكافئين . ومن تعريف التكافؤ تكون S_1 مكافئة لـــ S_2 ، بالرموز $S_1 \sim S_2$. وبالمثل فإن $S_3 \sim S_4$ ونبرهن على أن $S_2 \sim S_3$ كالآتى :

$$A_{r-1}/A_{r-1} \cap B_{s-1} \cong A_{r-1}B_{s-1}/B_{s-1} = G/B_{s-1}$$

وبالمثل فإن :

$$B_{s-1}/A_{r-1} \cap B_{s-1} \cong G/A_{r-1}$$

ومن ثم فإن $S_2 \sim S_3$. ولأن ~ علاقة تكافؤ فإن $S_1 \sim S_4$.

نهاية البرهان .

<u>٦-١-١٣ أمثلة محلولة</u> :

<u>مثال ١</u> : اضرب مثالاً لبيان أن متسلسلة التركيب لزمرة ما ليست بالضرورة وحيدة .

<u>الحل</u>: فى الزمرة الثمانية : $\{e\} \subset \{e,\alpha^2\} \subset \{e,\alpha,\alpha^2,\alpha^3\} \subset G$ ،

$$\{e\} \subset \{e,\beta\} \subset \{e,\alpha^2,\beta,\alpha^2\beta\}$$

متسلسلتا تركيب .

<u>مثال ٢</u>: طبق نظرية جوردان – هولدر على الزمر الدائرية المنتهية لتحقق وحدانية التحليل لعدد صحيح موجب إلى أعداد أولية موجبة .

<u>الحل</u> : ليكن n عدداً صحيحاً موجباً ، C زمرة دائرية منتهية رتبتها n . ولتكن

$$\{e\} \subset C_1 \subset \ldots \subset C_i = C \qquad (\text{العنصر المحايد فى } C \; e)$$

متسلسلة تركيب لـــ C . باستخدام نظرية جوردان – هولدر تكون الأعداد الأولية

$$p_1 = Ord(C_1), p_2 = Ord(C_2/C_1), \ldots, p_i = Ord(C_i/C_{i-1})$$

وحيدة . ولكن

$$(Ord(C) = Ord(C_i) = \frac{Ord(C_i)}{Ord(C_{i-1})} \cdot \frac{Ord(C_{i-1})}{Ord(C_{i-2})} \cdots \frac{Ord(C_2)}{Ord(C_1)} \cdot \frac{Ord(C_1)}{1}$$

$$= p_i p_{i-1} \ldots p_2 p_1 \; .$$

نهاية البرهان .

تذكر أن الزمرة G يقال إنها زمرة – p إذا كانت رتبة كل عنصر من عناصرها قوة من قوى p .

مثال ٣ : أذا كانت C زمرة دائرية لها متسلسلة تركيب وحيدة فإنها تكون زمرة $p-$.

البرهان : لتكن

$$\{e\} \subset C_1 \subset C_2 ... \subset C_{i-1} \subset C_i \subset C_{i+1} \subset ... \subset C_n = C \qquad (*)$$

متسلسلة تركيب لــ G ، وليكن

$$Ord(C_1) = p_1, Ord(C_{i+1}/C_i) = p_{i+1}, \ \ i = 1,2,...,n-1 \qquad \text{(أعداد أولية)}$$

ليكن $p_1 = ... = p_i$ ، $p_{i+1} \neq p_i$. لأن $Ord(C_{i+1}) = p_{i+1}p_i...p_1$ ، فإن C_{i+1} لها C_i' زمرة جزئية طبيعية عظمى من الرتبة $p_{i+1}p_{i-1}p_{i-2}...p_1$. عندئذ فإن :

$$Ord(C_{i+1}/C_i') = p_i, Ord(C_i'/C_{i-1}) = p_{i+1}$$

ومن ثم فإن :

$$\{e\} \subset C_1 \subset C_2 \subset ... \subset C_{i-1} \subset C_i' \subset C_{i+1} \subset ... \subset C_n = C$$

تكون متسلسلة تركيب مختلفة عن متسلسلة التركيب (*) . وهذا تناقض مع فرض وحدانية متسلسلات التركيب ، ومن ثم فإن $p_1 = p_2 = ... = p_n$ ، وتكون رتبة الزمرة C هى p^n ، وتكون رتبة كل عنصر من عناصرها قوة من قوى p .

مثال ٤ : برهن على أن أى زمرة إبدالية غير منتهية لايكون لها متسلسلة تركيب ($\mathbb{Z}$ على وجه الخصوص ليس لها متسلسلة تركيب).

البرهان : نلاحظ أولاً أن الزمرة الإبدالية البسيطة غير التافهة تكون دائرية وتتولد من أى عنصر فيما عدا العنصر المحايد (انظر (٤-١-١٠) ، (١-١١-٧) ، (١-١١-١١)) .

ومن ثم فإنه إذا كانت G زمرة إبدالية لها متسلسلة التركيب :

$$\{e\} \subset G_0 \subset G_1 \subset G_2 \subset ... \subset G_n = G$$

فإن عوامل التركيب G_i/G_{i-1} تكون دائرية ولها الرتب الأولية p_i ، $i = 1,...,n$ وعندئذ فإن $Ord(G) = p_1p_2...p_n$ ، أى أن G ينبغى لها أن تكون منتهية .

مثال ٥ : برهن على أن المتسلسلتين الطبيعيتين لـــ $\mathbb{Z}_{15}$:

$$\{\bar{0}\} \subset [\bar{5}] \subset \mathbb{Z}_{15} \;,$$

$$\{\bar{0}\} \subset [\bar{3}] \subset \mathbb{Z}_{15}$$

متكافئتان .

البرهان : (انظر مثال ١٦ من أمثلة محلولة (٣-١-١٣))

$\mathbb{Z}_{15}/[\bar{5}]$ ، $[\bar{3}]/[\bar{0}]$ متشاكلتان مع $\mathbb{Z}_5$ ، بينما $\mathbb{Z}_{15}/[\bar{3}]$ ، $[\bar{5}]/[\bar{0}]$ متشاكلتان مع $\mathbb{Z}_3$

مثال ٦ : برهن على أن $\mathbb{Z}$ ليس لها متسلسلة تركيب (انظر مثال ٤ أعلاه)

البرهان : لنفترض أن $\mathbb{Z}$ لها المتسلسلة الطبيعية :

$$\{0\} = H_0 \subset H_1 \subset \ldots \subset H_{n-1} \subset H_n = \mathbb{Z}$$

عندئذ فإن $H_1 = m\mathbb{Z}$ حيث $m \in \mathbb{N}$. وبالتالى فإن $H_1/H_0 \cong m\mathbb{Z}$ وهى زمرة دائرية غير منتهية، بها زمر جزئية طبيعية متعددة ، على سبيل المثال $2m\mathbb{Z}$. وبالتالى فإن $\mathbb{Z}$ لايكون لها متسلسلة تركيب.

مثال ٧ : حدد إذا ما كانت التقارير الآتية صحيحة أم خاطئة :

(أ) $\{0\} \subset 8\mathbb{Z} \subset 4\mathbb{Z} \subset \mathbb{Z}$ متسلسلة طبيعية للزمرة $\mathbb{Z}$ (تحت عملية الجمع)

(ب) $\{0\} \subset 9\mathbb{Z} \subset \mathbb{Z}$ متسلسلة طبيعية للزمرة $\mathbb{Z}$

(جـ) $\{(\bar{0},\bar{0})\} \subset [(\bar{0},\bar{3})] \subset [(\bar{0},\bar{1})] \subset [\bar{2}] \otimes [\bar{1}] \subset [\bar{1}] \otimes [\bar{1}] = \mathbb{Z}_4 \otimes \mathbb{Z}_9$

(د) كل زمرة إبدالية لها بالضبط متسلسلة تركيب وحيدة

(هـ) نظرية جوردان – هولدر لها نوع من التشابه مع النظرية الأساسية فى الحساب ، التى تقرر أن كل عدد صحيح موجب أكبر من 1 يمكن تحليله بطريقة وحيدة إلى حاصل ضرب أعداد أولية .

الحـــل : التقرير (د) خاطئ (انظر مثال ١). باقى التقارير صحيح .

٦-٢ الزمر القابلة للحل

٦-٢-١ تعريف : يقال لزمرة G إنها قابلة للحل (solvable) إذا كان لها متسلسلة طبيعية

$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_r = G$

بحيث إن G_i / G_{i-1} تكون إبدالية لجمع $i = 1, 2, \ldots, r$

٦-٢-٢ أمثلة :

(١) كل زمرة إبدالية تكون قابلة للحل . فإذا كانت G زمرة إبدالية وكان e عنصرها المحايد فإنه يمكن على الأقل كتابة المتسلسلة الطبيعية "التافهة" :

$$\{e\} = G_0 \subset G$$

حيث $G/\{e\}$ إبدالية (تذكر أن G ، $\{e\}$ زمرتان جزئيتان طبيعيتان تافهتان من G).

(٢) الزمرة $S_3 (= \gamma_3)$ قابلة للحل لأن

$\{e\} \subset \{e, (1\ 2\ 3), (1\ 3\ 2)\} \subset S_3$

متسلسلة طبيعية (تذكر أن $N := \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ هى الزمرة الجزئية الطبيعية غير التافهة الوحيدة من S_3) ، $S/N \cong \mathbb{Z}_2$ زمرة إبدالية (انظر مثال ٩ من أمثلة متنوعة على الباب الأول) ، $N/\{e\} \cong \mathbb{Z}_3$ أى زمرة إبدالية

(٣) S_4 قابلة للحل لأن :

$\{e\} \subset \{e, (1\ 2)(3\ 4)\} (=: N_1), \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} (=: N_2) \subset A_4 \subset S_4$

متسلسلة طبيعية ، N_2/N_1 ، A_4/N_2 ، S_4/A_4 زمر إبدالية ($N_1/\{e\}$ واضح أنها زمرة إبدالية).

والآن تذكر أن " الزمرة المشتقة G' من الزمرة G هى زمرة جزئية طبيعية من الزمرة G ، تتولد من الإبداليات $a^{-1}b^{-1}ab$ حيث $a, b \in G$. و G' لها الخاصة G/G' زمرة إبدالية ، وإذا كانت H زمرة جزئية طبيعية من G ، بحيث إن G/H إبدالية فإن $H \supset G'$. تسمى كذلك G' **زمرة الإبداليات** (commutator group) لـــ G .

سنعرف $G^{(0)} := G$ ، $G^{(1)} := G'$ ، $G^{(2)} := (G')'$ ، ... ، $G^{(m)} := (G^{(m-1)})'$

وبالتالى فإن كل $G^{(n)}$ تكون زمرة جزئية طبيعية من $G^{(n-1)}$ ، $G^{(n-1)}/G^{(n)}$ تكون زمرة إبدالية.

<u>٦-٢-٣ نظرية</u> : الزمرة G قابلة للحل إذا وفقط إذا وجد عدد طبيعى k : $k \in \mathbb{N} \setminus \{0\}$

بحيث إن $G^{(k)} = \{e\}$ (e عنصر G المحايد)

<u>البرهان</u> : لتكن G زمرة قابلة للحل . عندئذ فإنه توجد متسلسلة طبيعية

$$\{e\} = N_0 \subset N_1 \subset \ldots \subset N_{k-1} \subset N_k = G$$

بحيث إن N_i/N_{i-1} تكون إبدالية k ، $i = 1, 2, \ldots, k$.

والآن N_k/N_{k-1} إبدالية تقتضى أن $N_{k-1} \supset N_k' = G'$. كذلك فإن N_{k-1}/N_{k-2} إبدالية

تقتضى أن $N_{k-2} \supset N_{k-1}' \supset (G')' = G^{(2)}$. وبالاستمرار على هذه الشاكلة نصل إلى

$$\{e\} = N_0 \supset G^{(k)} \Rightarrow G^{(k)} = \{e\}$$

وبالعكس : ليكن $G^{(k)} = \{e\}$. لنعتبر السلسلة :

$$\{e\} = G^{(k)} \subset G^{(k-1)} \subset G^{(k-2)} \subset \ldots \subset G^{(1)} \subset G^{(0)} = G$$

هذه متسلسلة طبيعية بحيث إن $G^{(m)}/G^{(m+1)}$ كلها إبدالية ، حيث $m = 0, 1, \ldots, k-1$ ،

ومن ثم فإن G تكون قابلة للحل .

<u>٦-٢-٤ ملحوظات</u> :

(أ) أى زمرة جزئية من زمرة قابلة للحل تكون قابلة للحل

(ب) لتكن G زمرة قابلة للحل ، ولتكن H زمرة جزئية طبيعية من G . عندئذ فإن G/H تكون قابلة للحل كذلك

(جـ) إذا كانت H زمرة جزئية طبيعية من G بحيث إن H ، G/H قابلتان للحل ، فإن G تكون قابلة للحل

البرهان : (أ) لتكن H زمرة جزئية من زمرة قابلة للحل G . واضح أن :

$$H \subset G \Rightarrow H^{(1)} \subset G^{(1)} \Rightarrow H^{(2)} \subset G^{(2)} \Rightarrow \dots \Rightarrow H^{(k)} \subset G^{(k)} \Rightarrow \dots$$

ولأن G قابلة للحل فإنه لعدد صحيح موجب k سيحدث أن $G^{(k)} = \{e\}$ وهكذا فإن $H^{(k)} = \{e\}$ ، أى أن H قابلة للحل .

(ب) ليكن $\bar{G} := G/H$. لكل $a,b \in G$:

$$(a^{-1}b^{-1}ab)H = (a^{-1}H)(b^{-1}H)(aH)(bH) = (aH)^{-1}(bH)^{-1}(aH)(bH)$$

ومن ثم فإن : $\bar{G}' = (\bar{G})'$ ، أى أن : $\overline{G^{(1)}} = (\bar{G})^{(1)}$. وبالاستقراء الرياضى ينتج أن :

$$\overline{G^{(k)}} = (\bar{G})^{(k)}$$

ولأن G قابلة للحل فإنه يوجد عدد صحيح موجب n بحيث إن $G^{(n)} = \{e\}$ حيث e عنصر G المحايد. ومن هذا ينتج أن $(\bar{G})^n = \{\bar{e}\}$ ، أى أن $\bar{G}$ قابلة للحل

(جـ) لتكن

$$\{e\} =: H_0 \subset H_1 \subset \dots \subset H_{n-1} \subset H_n = H$$

متسلسلة طبيعية لـ H بحيث إن H_i/H_{i-1} تكون إبدالية ، $i = 1, \dots, n$. ولتكن

$$H/H =: G_0/H \subset G_1/H \subset G_2/H \subset \dots \subset G_{m-1}/H \subset G_m/H = G/H$$

متسلسلة طبيعية لـ G/H بحيث إن :

$$\frac{G_i/H}{G_{i-1}/H} \cong G_i/G_{i-1}$$

تكون إبدالية ، $i = 1, \dots, m$. عندئذ يكون لدينا :

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \dots \subset H_{n-1} \subset H_n = H = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_{m-1} \subset G_m = G$$

وهى متسلسلة طبيعية ، ونظراً لأن H_i/H_{i-1} ، G_j/G_{j-1} إبدالية ، $i = 1, \dots, n$ ، $j = 1, \dots, m$ ، تكون G قابلة للحل .

٦-٢-٥ نظرية : أى زمرة منتهية قابلة للحل G لها متسلسلة تركيب

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G$$

بحيث إن عوامل التركيب G_i / G_{i-1} تكون زمراً دائرية لها رتب هى أعداد أولية ، $i = 1, \ldots, n$.

البرهان : بالاستقراء الرياضى على رتبة (G) . إذا كان $Ord(G) = 1$ أو كانت G بسيطة يكون الادعاء صحيحاً . لنفترض أن الادعاء صحيح لجميع الزمر التى لها رتبة أقل من $Ord(G)$ ، G ليست بسيطة . إذا كانت H زمرة جزئية طبيعية غير تافهة من G، فإنه من فرض الاستقراء يكون لـــ H ، G/H متسلسلتا تركيب مع عوامل تركيب هى زمر دائرية رتبها أعداد أولية . ونصل إلى المطلوب مثلما فى (٦-٢-٤) (جـــ) .

٦-٢-٦ أمثلة محلولة :

مثال ١ : برهن على أن $S_n (= \gamma_n), n \geq 5$ ليست قابلة للحل .

البرهان : لتكن N زمرة جزئية طبيعية من $G = S_n$ ، $n \geq 5$ ولتكن N تحتوى على كل الدورات ذات الطول 3 فى S_n . سنبرهن على أن N' زمرة الإبدال لـــ N (= الزمرة المشتقة من N) تحتوى على جميع الدورات ذات الطول 3 كالآتى :

ليكن $a = (1\ 3\ 2)$ ، $b = (3\ 5\ 4)$ عنصرين فى N . عندئذ فإن :

$$a^{-1}b^{-1}ab = (1\ 2\ 3)(3\ 4\ 5)(1\ 3\ 2)(3\ 5\ 4) = (3\ 1\ 4) = (1\ 4\ 3) \in N'$$

ولدينا N' زمرة جزئية طبيعية من S_n

وهكذا فإنه لأى $\sigma \in S_n$ يكون : $\sigma^{-1}(1\ 4\ 3)\sigma \in N'$

نختار $\sigma \in S_n$ بحيث يكون : $\sigma(1) = i_1$ ، $\sigma(4) = i_2$ ، $\sigma(3) = i_3$ حيث $(i_1\ i_2\ i_3)$ دورة اختيارية فى S_n طولها 3 . وبالتالى يكون بحساب بسيط :

$$\sigma^{-1}(1\ 4\ 3)\sigma = (i_1\ i_2\ i_3)$$

أى أن $(i_1\ i_2\ i_3)$ عنصر فى N' . والآن ضع $N = G$ عندئذ فإن G' تحتوى على كل الدورات ذات الطول 3 . ونظراً لأنه لجميع $k \in \mathbb{N}$ تكون $G^{(k)}$ زمرة جزئية طبيعية من G ، فإنه بتكرار تطبيق ماسبق تكون $G^{(k)}$ محتوية على جميع الدورات ذات الطول 3 ، وبهذا تكون $G^{(k)} \neq \{e\}$ ، لأى عدد صحيح موجب k ، أى أن G ليست قابلة للحل.

<u>مثال ٢</u> : برهن على أن الزمرة المتغيرة $A_n, n \geq 5$ بسيطة .

<u>البرهان</u> : لتكن H زمرة جزئية طبيعية من A_n . سنبرهن أولاً على أنه إذا كانت $H \neq \{e\}$ فإن H تحتوى على دورة طولها 3 . لتكن α تبديلة فى H ولا تساوى $\{e\}$ بحيث إنها تترك أكبر عدد من العناصر فى $\{1, 2, \ldots, n\}$ ثابتاً . إذا لم تكن α دورة طولها 3 ، فإنها إما أن تحتوى على دورة طولها أكبر من أو يساوى 3 ، وإما أن α هى حاصل ضرب نقلتين (تحويلتين) منفصلتين على الأقل ، أى أن α إما :

(1) $\alpha = (1\ 2\ 3\ \ldots)\ (\ldots\ldots)\ \ldots,$

وإما

(2) $\alpha = (1\ 2)(3\ 4)\ \ldots$

فى الحالة الأولى "ستحرك " على الأقل رقمين آخرين وليكونا 4 ، 5 ، لأن α ليست واحدة من التبديلات الفردية التى لها الشكل $(1\ 2\ 3\ k)$. والآن لتكن $\beta = (3\ 5\ 4)$ ، ولتكن $\gamma = \beta^{-1}\alpha\beta$. فإذا كانت α كما فى (1) فإن $\gamma = (1\ 2\ 4\ \ldots)\ \ldots$ ؛ أما إذا كانت α كما فى (2) فإن $\gamma = (1\ 2)(4\ 5)\ \ldots$.

علاوة على هذا فإنه إذا كان رقم $i > 5$ ترك ثابتاً بـــ α فإنه سيترك ثابتاً أيضاً بـــ γ وبالتالى يترك ثابتاً كذلك بـــ $\alpha^{-1}\gamma$. وأكثر من هذا فإن $\alpha^{-1}\gamma(1) = 1$ إذا كانت α كما هى فى (1) ، كذلك $\alpha^{-1}\gamma(1) = 1$ ، $\alpha^{-1}\gamma(2) = 2$ إذا كانت α مثلما هى فى (2) .

وهكذا فإن $\alpha^{-1}\gamma$ تترك عدداً ثابتاً من العناصر أكبر من الذى تتركه α ، وهذا يناقض اختيار α . ومن ثم فإن α دورة ذات الطول 3 . ويكمل البرهان باستخدام نفس النقاش

فى مثال ١ مع مراعاة مثال ١٨ فى الباب الثانى فيكون $H = A_n$ ، ومن ثم فإن A_n تكون زمرة بسيطة .

حل آخر : للبرهنة على أن A_5 بسيطة سنبرهن اولاً على التمهيدية الآتية :

لتكن N زمرة جزئية طبيعية من زمرة منتهية G . إذا كان

$gcd(Ord(x), Ord(G/H)) = 1$ فإن $x \in H$

<u>البرهان</u>: $gcd(Ord(x), Ord(G/H)) = 1$ يقتضى أن $gcd(Ord(xH), Ord(G/H)) = 1$.

ولكن $Ord(xH)$ يقسم $Ord(G/H)$ (١-١١-٩) (٢) . ومن ثم فإن $Ord(xH) = 1$ أى أن $Ord(xH) = H$ وبالتالى فإن $x \in H$.

والآن : لتكن A_5 تحتوى على زمرة جزئية طبيعية غير تافهة H . عندئذ فإن $Ord(H) = 2, 3, 4, 5, 6, 10, 12, 15, 20$ أو 30 . ويمكن التأكد من أن A_5 تحتوى على 24 عنصراً من الرتبة 5 ، 20 عنصراً من الرتبة 3، ولاتحتوى على أية عناصر من الرتبة 15 . إذا كانت رتبة (H) هى 3 أو 6 أو 12 أو 15 فإن $gcd(Ord(A_5/H), 3) = 1$ ومن التمهيدية السابقة ستحتوى H على كل العناصر العشرين ذوى الرتبة 3 . أما إذا كانت رتبة (H) هى 5 أو 10 أو 20 فإن $gcd(Ord(A_5/H), 5) = 1$ وبهذا ستحتوى H على جميع العناصر الأربعة وعشرين من الرتبة 5 . أما إذا كانت رتبة (H) هى 30 فإن $gcd(Ord(A_5/H), 3) = 1$ ،

$gcd(Ord(A_5/H), 5) = 1$ ، وبهذا تحتوى H على كل العناصر من الرتبة 3 ، الرتبة 5 .

وأخيراً إذا كانت رتبة (H) هى 2 أو 4 فإن رتبة (A_5/H) هى 30 أو 15 . توجد زمرة وحيدة من الرتبة 15 هى $\mathbb{Z}_{15}$ فيها $\bar{1}$ من الرتبة 15 ، كذلك أى زمرة من الرتبة 30 تحتوى على عنصر من الرتبة 15 . لكن A_5 لاتحتوى على عنصر من الرتبة 15 ، وبالتالى فإن A_5/H لاتحتوى على مثل هذا العنصر .

ومن ثم البرهان .

<u>مثال ٣</u> : برهن على أن G أى زمرة بسيطة وغير إبدالية تكون غير قابلة للحل .

<u>البرهان</u> : فى هذه الحالة يكون لدينا المتسلسلة الطبيعية التافهة الآتية فقط :

$$\{e\} \subset G$$

لكن $G/\{e\}$ ليست إبدالية وبهذا تكون G غير قابلة للحل .

طريقة أخرى : نعلم أن G' زمرة جزئية طبيعية فى G . ومن حيث إن G بسيطة فهناك بالضبط إمكانيتان :

1) $G' = \{e\} \Rightarrow \forall a,b \in G : a^{-1}b^{-1}ab = e \Rightarrow \forall a,b \in G : ab = ba$

$\Rightarrow G$ إبدالية : وهذا تناقض

2) $G' = G \quad \Rightarrow \quad G = G^{(n)} \neq \{e\} \quad \forall n \in \mathbb{N}$

الاستقراء الرياضى

أى أن G ليست قابلة للحل (٦-٢-٣)

مثال ٤ : باستخدام مثالى (٢) ، (٣) السابقين برهن على أن S_n ليست قابلة للحل إذا كان $n \geq 5$ (قارن مع مثال١)

البرهان : من مثال٢ نعلم أن A_n بسيطة إذا كان $n \geq 5$ ، A_n عندما $n \geq 5$ تكون غير إبدالية فمن مثال ٣ تكون A_n غير قابلة للحل، ومن (٦-٢-٤) تكون S_n غير قابلة للحل .

مثال ٥ : برهن على أن $\{e\} \subset A_n \subset S_n (= \gamma_n)$ حيث $n \geq 5$ متسلسلة تركيب لـــ S_n . (e هو العنصر المحايد فى S_n)

البرهان : $A_n/\{e\}$ متشاكلة مع A_n ، A_n بسيطة ، حيث $n \geq 5$ (مثال٢ أعلاه) . كذلك فإن S_n/A_n متشاكلة مع $\mathbb{Z}_2$ ، أى هى بسيطة .

تمارين

(١) باستخدام (٢-١-١٤) برهن على الآتى :

الزمرتان A_n ، γ_n حيث $n \geq 5$ ليستا قابلتين للحل .

(٢) باستخدام تمارين الباب الثانى برهن على أن A_2 ، A_3 ، γ_2 ، γ_3 قابلة للحل

(٣) مستخدماً نظرية لاجرانج برهن على أن γ_3 قابلة للحل

(٤) برهن حسابياً على أن A_4 ، γ_4 قابلتان للحل

(٥) برهن على أنه إذا كانت الزمرة المنتهية G تحتوى على زمرة جزئية دليلها فى G يساوى 2 ، فإن G ليست بسيطة

(٦) برهن أو انف

(أ) كل زمرة منتهية لها متسلسلة تركيب .

(ب) S_7 قابلة للحل

(جـ) كل زمرة منتهية ، رتبتها عدد أولى تكون قابلة للحل

(٧) اوجد متسلسلة تركيب لـ $S_3 \times S_3$. هل $S_3 \times S_3$ قابلة للحل ؟

(٨) اوجد جميع متسلسلات التركيب لـ $\mathbb{Z}_{60}$ ، وبرهن على أنها جميعا متشاكلة .

(٩) اوجد جميع متسلسلات التركيب لـ $\mathbb{Z}_5 \otimes \mathbb{Z}_5$

(١٠) اوجد جميع متسلسلات التركيب لـ $\mathbb{Z}_3 \otimes \mathbb{Z}_2$

2 Ring Theory نظرية الحلقات

القسم



١-١ الحلقات

١-١-١تعريف : يسمى الثلاثى (.,+,R) المكون من مجموعة غير خالية R .

عمليتين + ، . ، **حلقة** (ring) إذاكان (وفقط إذا كان) :

(أ) $(R, +)$ زمرة إبدا لية (commutative group)

(ب) العملية "." تشاركية (أو إدماجية أو تجميعية) (associative) أى أنه لكل $a,b,c \in R$:

$(a.b).c = a(b.c)$

(جـ) قانونا التوزيع متحققين أى أنه لكل $a,b,c \in R$:

$$a.(b+c) = a.b + a.c,$$

$$(a+b)c = a.c + b.c$$

١-١-٢ ملحوظة : سنكتب عادة R بدلاً من (.,+,R) . وسنكتب غالباً ab بدلاً من $a.b$. تسمى الزمرة $(R, +)$ الزمرة الجمعية (additive group) للحلقة R . وسنشير إلى عنصرها المحايد بالرمز "0" ويسمى **صفر الحلقة** (The zero element of the ring) أو **العنصر الصفرى للحلقة** (لاحظ أنه وحيد كما سبق فى نظرية الزمر). وفيما يلى **سنعنى بـــ R دائما حلقة** إذا لم ينص على غير ذلك .

١-١-٣ تعريف :(أ) يقال للحلقة R إنها **إبدالية** (commutative) إذا كان لكل $a,b \in R$:

$$ab = ba$$

(ب) يقال لعنصر $1 \in R$ إنه **عنصر الوحدة** (unity) إذا كان لكل $a \in R$:

$$1a = a = a1$$

(لاحظ أنه **وحيد** لأنه إذا كان هناك $1,1'$ وكلاهما عنصر وحده فإن : $1 = 1.1' = 1'$

(جـ) سنعرف قوى عنصر $a \in R$ استقرائياً كالاتى :

$$a^1 := a, \quad a^n := aa^{n-1}$$

لجمع $n \in \mathbb{N}$ ، $n \geq 2$.

وإذا كان $1 \in R$ فإننا نعرف $a^0 := 1$.

١-١-٤ قواعد الحساب : لكل $a,b\in R$:

(أ) $a0=(0+0)a=0a+0a$

$$\Rightarrow \underline{0}=-0a+0a=-0a+(0a+0a)=(-0a+0a)+0a=0+0a=\underline{0a}$$

وبالمثل $a\,0=0$

(ب) $0=0b=(-a+a)b=(-a)b+ab$

$$\Rightarrow -(ab)=0+(-(ab))=(-a)b+ab+(-(ab))=(-a)b+(ab+(-ab))$$
$$=(-a)b+0=(-a)b$$

وبالمثل $-(ab)=a(-b)$

وينتج مباشرة أن : $(-a)(-b)=ab$

(جـ) بالاستقراء الرياضى يمكن البرهنة بسهولة على أنه لجميع $a\in R$ ، ولجميع $m,n\in\mathbb{N}\setminus\{0\}$:

$$a^m.a^n=a^{m+n}\quad,\quad (a^m)^n=a^{mn}$$

١-١-٥ ملحوظة : ليكن $1\in R$ عنصر الوحدة ، ولتكن $R\neq\{0\}$. عندئذ فإن: $1\neq 0$ وإلا :

تناقض $1=0\Rightarrow a=1a=0a=0\Rightarrow R=\{0\}$

١-١-٦ تعريف : (أ) يقال لعنصر $a\in R$ إنه **قاسم صفرى أيمن** (right zero divisor) (**أيسر**) (left) لـ R إذا وجد $x\in R\setminus\{0\}$ بحيث إن $xa=0$ $(ax=0)$

(ب) يقال للحلقة R إنها **خالية من القواسم الصفرية** (has no zero divisors) إذا كانت لاتحتوى على قواسم صفرية يمنى أو يسرى .

١-١-٧ تعريف : لتكن R حلقة بها $R\ni 1\neq 0$. يقال إن R **نطاق متكامل** (integral domain) إذا كانت R إبدالية وخالية من القواسم الصفرية . (رأينا فى (١-١-٥) أن $(R=\{0\}\Leftarrow 0=1\in R$

١-١-٨ تعريف : لتكن R حلقة وليكن $R\ni 1\neq 0$. يقال لعنصر $a\in R$ إنه **وحدة** (unit) إذا وجد عنصران $a,c\in R$ بحيث إن :

$$ab=1=ca$$

سنرمز لمجموعة الوحدات فى R بالرمز R^* .

لاحظ الفرق بين التعريفين : "عنصر الوحدة" ، "وحدة" .

<u>١-١-٩ ملحوظة</u> : لتكن R حلقة ، $R \ni 1 \neq 0$.

(أ) R^* لاتحتوى على قواسم صفرية يمنى أو يسرى .

(ب) لتكن $a,b,c \in R$ ، $a \in R^*$ ، $ab = 1 = ca$. ينتج أن $b = c$

<u>البرهان</u> : (أ) ليكن $a \in R^*$ قاسماً صفرياً أيسر . عندئذ فإنه يوجد $b,c \in R$ ، $b \neq 0$ بحيث إن

$ab = 0 \, , \; ca = 1$. عندئذ فإن :

$$0 = c(ab) = (ca)\,b = 1\,b = b \quad \text{تناقض}$$

وبالمثل يثبت أنه لايوجد فى R^* قاسم صفرى أيمن .

(ب) $b = 1\,b = (ca)\,b = c(ab) = c\,1 = c$

<u>١-١-١٠ ملحوظة</u> : لتكن R حلقة ، $R \ni 1 \neq 0$

(أ) $a,b \in R^* \;\Leftarrow\; ab \in R^*$

(ب) المجموعة R^* مع العملية المستحدثة (The induced operation) $R^* \times R^* \to R^*$ ، $(a,b) \mapsto ab$ تكون زمرة .

<u>البرهان</u> : (أ) $a,b \in R^* \Rightarrow \exists c,d \in R : ca = ac = 1, db = bd = 1$

$$\left.\begin{array}{l} \Rightarrow \;\; (ab)(dc) = a(bd)c = a1c = ac = 1, \\ \qquad (dc)(ab) = d(ca)b = d1b = db = 1 \end{array}\right\rangle \; ab \in R^*$$

(ب) واضح أن العملية المستحدثة تشاركية (إدماجية ، تجميعية) لأن العملية الأصلية كذلك . كذلك فإنه من الواضح أن $1 \in R^*$. يتبقى أن نثبت أنه لكل $a \in R^*$ يوجد $b \in R^*$ بحيث إن $ba = 1 (= ab)$ ولكن هذا أيضاً واضح من تعريف R^* (بدهى أنه إذا كان $a \in R^*$ فإنه يوجد $b \in R^*$ بحيث إن $ba = ab = 1$) .

١-١-١١ تعريف : تسمى الحلقة $(R, +, .)$ **شبه حقل** (skew field) إذا حققت :

(أ) R خالية من القواسم الصفرية ، أى أن $a,b \in R\setminus\{0\} \Leftarrow ab \in R\setminus\{0\}$ أى أن الضرب المستحدث من الضرب "." فى R سيكون عملية فى R^*

(ب) المجموعة $R\setminus\{0\}$ مع الضرب المستحدث (أى الضرب "." محدداً على $R\setminus\{0\}$ تكون زمرة . (لاحظ أن هذا يتضمن أن $R \ni 1 \neq 0$) إذا تحقق فى شبه الحقل R أنه إبدالى أى أنه لكل $a,b \in R$ يكون $ab = ba$ فإن شبه الحقل يكون **حقلاً** (field) .

١-١-١٢ ملحوظة: R حلقة ، $R \ni 1 \neq 0$. R شبه حقل إذا كان وفقط إذا كان $R^* = R\setminus\{0\}$

١-١-١٣ نظرية : كل نطاق متكامل منته (finite) يكون حقلاً .

البرهان : ليكن R نطاقاً متكاملاً منتهياً . المطلوب البرهنة على أن $R\setminus\{0\} \subset R^*$ (بدهى أن $R^* \subset R\setminus\{0\}$) . ليكن $a \in R\setminus\{0\}$. الراسم

$$\ell_a : R \to R,$$
$$x \mapsto ax$$

راسم أحادى (واحد لواحد) لأن :

$$\forall x, y \in R : \ell_a(x) = \ell_a(y) \Rightarrow ax = ay \Rightarrow a(x-y) = 0$$
$$\Rightarrow \quad x - y = 0 \Rightarrow x = y$$

$a \neq 0,$

R خالية من القواسم الصفرية لأنها نطاق متكامل

ولكن R منته ، إذن ℓ_a راسم غامر (شامل ، فوقى) وهذا يقتضى أنه يوجد $z \in R$ بحيث إن $az = \ell_a(z) = 1$ أى أن $a \in R^*$ وبالتالى R يكون حقلاً .

(لاحظ أن $1 \in R$ لأن R نطاق متكامل ، $a \in R^*$ معناه أن a له معكوس ضربى ، أى معكوس بالنسبة لعملية الضرب ".")

١-١-١٤ أمثلة للحلقات:

مثال ١ : مجموعة الأعداد الصحيحة $\mathbb{Z}$ مع عمليتى الجمع والضرب العاديتين تكون حلقة لها عنصر الوحدة 1، وهى حلقة إبدالية ولها وحدتان1 ، 1 - . (هى نطاق متكامل).

مثال ٢ : المجموعة $\mathbb{Z}[X]$: مجموعة كثيرات الحدود ذات المعاملات الصحيحة فى المتغير X مع عمليتى الجمع والضرب العاديتين تكون حلقة إبدالية ولها عنصر الوحدة 1 . (هى نطاق متكامل)

مثال ٣ : المجموعة $M_{2\times2}(\mathbb{Z})$: مجموعة المصفوفات المربعة من النوع 2×2 وعناصرها (عناصر أى مصفوفة منها) أعداد صحيحة تكون حلقة لها عنصر الوحدة $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ وهى غير إبدالية .

مثال ٤ : المجموعة $2\mathbb{Z}=\{...,-4,-2,0,2,4,...\}$: مجموعة الأعداد الزوجية مع عمليتى الجمع والضرب العاديتين تكون حلقة إبدالية وليس لها عنصر الوحدة .

مثال ٥ : $\mathbb{Q}$ مجموعة الأعداد النسبية (الكسرية) ، $\mathbb{R}$ مجموعة الأعداد الحقيقية ، $\mathbb{C}$ مجموعة الأعداد المركبة مع عمليتى الجمع والضرب العاديتين تكون حلقات إبدالية ولها عنصر الوحدة 1 . (هى كلها حقول).

مثال ٦ : لتكن X مجموعة غير خالية ، R حلقة . لتكن $Map(X,R)$ هى مجموعة جميع الرواسم من X إلى R مع العمليتين "+" ، "." المعرفتين كالآتى :

$$(f \dot{+} g)(x) := f(x) \dot{+} g(x)$$

هذه المجموعة مع العمليتين المذكورتين تكون حلقة إبدالية إذا كانت R إبدالية . وإذا كانت R لها عنصر الوحدة "1" فإن الراسم $\begin{matrix} f: X\to R \\ x\mapsto 1\end{matrix}$ يكون هو عنصر الوحدة فى $Map(X,R)$.

مثال ٧ : لتكن X فراغاً توبولوجيا : $C(X,\mathbb{R})$ مجموعة جميع الدوال المتصلة من X إلى $\mathbb{R}$. ولتكن العمليتان معرفتين كما هما فى مثال ٦ ، عندئذ فإن $C(X,\mathbb{R})$ مع العمليتين تكون حلقة إبدالية ذات عنصر وحدة .

مثال ٨ : لتكن X مجموعة جزئية غير خالية من $\mathbb{C}$ ، ولتكن $\theta(X)$ مجموعة جميع الدوال الهولومورفية (التحليلية ، القابلة للتفاضل) المعرفة على X . ولتكن العمليتان "+" ، "." معرفتين مثلما فى مثال ٦ . عندئذ فإن $\theta(X)$ مع العمليتين تكون حلقة إبدالية ذات عنصر وحدة .

مثال ٩: لتكن $(G, +)$ زمرة إبدالية ، وليكن 0 هو عنصرها المحايد . سنعرف العملية "." على G كالآتى :

$$\forall a,b \in G: \quad a.b = 0$$

عندئذ فإن $(G, +, .)$ تكون حلقة إبدالية .

وإذا كانت $G = \{0\}$ تسمى هذه الحلقة الحلقة الصفرية . أما إذا كانت $G \neq \{0\}$ فواضح أن G ليس لها عنصر الوحدة .

مثال ١٠ : المجموعة $\mathbb{Z}_n = \{0,1,...,n-1\}$ مع عمليتى الجمع والضرب مقياس n (modulo n) تكون حلقة إبدالية لها عنصر الوحدة 1 . ووحداتها هى المجموعة $U(n)$.

١-١-١٥ أمثلة محلولة :

مثال ١ : برهن على أن الراسمين

$$\ell_a : R \to R \ , \quad r_a : R \to R$$
$$x \mapsto ax \qquad x \mapsto xa$$

أندومورفيزمان للزمرة $(R, +)$ ، حيث $(R, +, .)$ حلقة

البرهان :

$$\forall x, y \in R: \quad \ell_a(x+y) := a(x+y)$$
$$= ax + ay = \ell_a(x) + \ell_a(y)$$

قانون التوزيع

وبالمثل :

$$\forall x, y \in R: \quad r_a(x+y) = (x+y)a \quad = \quad xa + ya = r_a(x) + r_a(y)$$

قانون التوزيع

مثال ٢ : لتكن X مجموعة بها على الأقل عنصران . برهن على أن الحلقة $Map(X,R)$ ليست خالية من القواسم الصفرية

الحل : ليكن $a,b\in X$ ، $a\neq b$. سنعرف $f,g:X\to\mathbb{R}$ بالكيفية الآتية :

$$f(a)=g(b)=0,$$
$$f(b)=g(a)=1,$$
$$f(x)=g(x)=0 \quad \forall x\in X\setminus\{a,b\}$$

عندئذ فإن : $f\neq\hat{0}\neq g$ ($\hat{0}$ هو الراسم الصفرى) لكن $fg=\hat{0}$.

مثال ٣ : برهن على أن لجميع $n\in\mathbb{N}$ ، $n\geq 2$ تكون الحلقة $M_{n\times n}(\mathbb{R})$ ليست خالية من القواسم الصفرية .

البرهان :

$$\left(\begin{array}{cc|c} 0 & 0 & \\ 0 & 1 & 0 \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right)\left(\begin{array}{cc|c} 0 & 1 & \\ 0 & 0 & 0 \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right)=\left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & 0 \end{array}\right)$$

مثال ٤ : لتكن $\phi\neq X\subset\mathbb{C}$ مجموعة جزئية مفتوحة (open) . برهن على أن الحلقة $\theta(X)$ (انظر مثال ٨ (١-١-١٤)) تكون خالية من القواسم الصفرية إذا كانت وفقط إذا كانت X مترابطة (connected) .

البرهان : لتكن X ليست مترابطة. عندئذ فإنه توجد مجموعتان مفتوحتان غير خاليتين U ، V من X بحيث يكون : $U\cup V=X$ ، $U\cap V=\phi$. نعرف :

$$f(x):=\begin{cases}0, & x\in U\\ 1, & x\in V\end{cases} \quad , \quad g(x):=\begin{cases}1, & x\in U\\ 0, & x\in V\end{cases}$$

وهما دالتان تحليليتان (قابلتان للتفاضل) $f,g : X \to \mathbb{C}$ بحيث إن $f \neq \hat{0} \neq g$ ($\hat{0}$ الدالة الصفرية) بينما $fg = \hat{0}$. إذن $\theta(X)$ ليست خالية من القواسم الصفرية .

والآن لنفترض أن $f,g \in \theta(X)$ مع $g \neq \hat{0}$ ، $fg = \hat{0}$. ومن ثم فلأن $g \neq \hat{0}$ فإنه يوجد $x \in X$ بحيث $g(x) \neq 0$. ولأن g متصلة فإنه يوجد جوار مفتوح (open neighborhood) U حول x بحيث إن $g(U) \neq 0$ لجميع $u \in U$ ولأن $fg = \hat{0}$ فإنه ينتج أن $f \,|\, U = \hat{0}$ (f محددة على $U = 0$) . ولأن f تحليلية ، X مترابطة ينتج من نظرية الدوال التحليلية أن $f = \hat{0}$.

مثال ٥ : برهن على أن مجموعة الإندومورفيزمات لزمرة إبدالية تكون حلقة .

البرهان : لتكن G زمرة إبدالية . سنشير إلى العملية فى G بالرمز "+" ، وسنشير إلى مجموعة كل الإندومورفيزمات لـــ G بالرمز Σ .

والآن ليكن $f : G \to G$ إندومورفيزماً ، فيكون

$$\forall a,b \in G: \quad f(a+b) = f(a) + f(b)$$

والآن نعرف عمليتين على Σبحيث تكون Σحلقة. سنعرف العملية الأولى"الجمع" كالآتى:

$$+ : \Sigma \times \Sigma \to \Sigma$$
$$(f,g) \mapsto f + g$$

حيث

$$\forall a \in G: \quad (f+g)(a) := f(a) + g(a)$$

سنبرهن الآن على أن $f+g$ إندومورفيزم لـــ G (f ، g إندومورفيزمان لـــ G) كالآتى :

$$\forall a,b \in G : (f+g)(a+b) := f(a+b) + g(a+b) \underset{f,g \in \Sigma}{=} f(a) + f(b) + g(a) + g(b)$$

$$= \quad f(a) + g(a) + f(b) + g(b) =: (f+g)(a) + (f+g)(b)$$

G إبدالية

والآن نعرف العملية الثانية "التركيب" كالآتى :

$$o:\Sigma\times\Sigma\to\Sigma$$
$$(f,g)\mapsto fog$$

حيث

$$\forall a\in G:\ \ (fog)(a):=f(g(a))$$

ونبرهن الآن على أن العملية "o" معرفة جيداً : أى أننا نبرهن على أن $f\ o\ g$ إندومورفيزم لـــ G (حيث f ، g إندومورفيزمان لـــ G) كالآتى :

$$\forall a,b\in G:(fog)(a+b):=f(g(a+b))\underset{g\in\Sigma}{=}f(g(a)+g(b))$$
$$\underset{f\in\Sigma}{=}f(g(a))+f(g(b))=:(fog)(a)+(fog)(b)$$

والآن :

(١)

$$\forall a\in G\ \ \ \forall f,g,h\in\Sigma\ :$$
$$((f+g)+h)(a):=(f+g)(a)+h(a):=(f(a)+g(a))+h(a)\ \ \underset{\text{زمرة } G}{=}\ \ f(a)+(g(a)+h(a))$$
$$=:f(a)+(g+h)(a)=:(f+(g+h))(a)\Rightarrow\forall f,g,h\in\Sigma:(f+g)+h=f+(g+h)$$

(٢) نعرف صفر الحلقة ونشير إليه بالرمز "0" كالآتى :

$$0:G\to G$$
$$a\mapsto o$$

حيث "0" هو العنصر المحايد فى G . سنبرهن على أن 0 معرف جيداً ، أى نبرهن على أنه إندومورفيزم وأنه لجميع $f\in\Sigma$ يكون $0+f=f$ كالآتى :

$$\forall a,b\in G:0(a+b):=0=0+0=:0(a)+0(b)$$

أى أن 0 إندومورفيزم والآن :

$$\forall f\in\Sigma\ \forall a\in G:(0+f)(a):=0(a)+f(a)=0+f(a)$$
$$=f(a)\Rightarrow 0+f=f$$

(٣) لكل $f \in \Sigma$ نعرف معكوس f بالنسبة للعملية "+" ونشير إليه بالرمز $-f$ كالآتى :

$$-f : G \to G$$
$$a \mapsto -f(a)$$

سنبرهن على أن $-f$ معرف جيداً أى أنه إندومورفيزم وأن $-f+f=0$ كالآتى :

$$\forall a,b \in G : (-f)(a+b) := -f(a+b) \underset{f\in\Sigma}{=} = -(f(a)+f(b))$$

$$= -f(b) - f(a) \quad = \quad -f(a) - f(b) =: (-f)(a) + (-f)(b)$$

G إبدالية

أى أن $-f$ إندومورفيزم ، والآن :

$$\forall a \in G : (-f+f)(a) := (-f)(a) + f(a) = -f(a) + f(a) = 0 = 0(a)$$

$$\Rightarrow -f + f = 0$$

أى أن $-f$ هو معكوس f (بالنسبة للعملية +)

(٤)

$$\forall f, g \in \Sigma \ \forall a \in G : (f+g)(a) := f(a) + g(a)$$

$$= \quad g(a) + f(a) =: (g+f)(a) \Rightarrow \forall f, g \in G : f+g = g+f$$

G إبدالية

(٥)

$$\forall f, g, h \in \Sigma : (fog)oh = fo(goh)$$

هذا صحيح لجميع الرواسم f ، g ، h مادام التركيب "o" معرفة .

(٦)

$$\forall f, g, h \in \Sigma \quad \forall a \in G :$$

$$((f+g)oh)(a) := (f+g)(h(a)) := f(h(a)) + g(h(a))$$

$$=: (foh)(a) + (goh)(a) =: (foh + goh)(a) \Rightarrow \forall f, g, h \in \Sigma : (f+g)oh = foh + goh,$$

$$(fo(g+h))(a) := f((g+h)(a)) := f(g(a)+h(a)) \underset{f\in\Sigma}{=} f(g(a)) + f(h(a))$$

$=: (fog)(a) + (foh)(a) =: (fog + foh)(a)$

$\Rightarrow \forall f, g, h \in \Sigma : fo(g+h) = fog + foh$

(٧) $\hat{1}$ هو عنصر الوحدة فى الحلقة Σ المعرف كالآتى :

$$\forall a \in G : \quad \hat{1}(a) := a$$

نبرهن على $\hat{1}$ معرف جيداً ، أى أنه بالفعل إندومورفيزم ، كما أنه

$$\forall f \in \Sigma \quad \hat{1} of = f, \qquad fo\hat{1} = f$$

كالآتى :

$$\forall a, b \in G : \hat{1}(a+b) := a + b =: \hat{1}(a) + \hat{1}(b)$$

أى أن $\hat{1}$ إندومورفيزم . والآن :

$$\forall f \in \Sigma \quad \forall a \in G: \quad (\hat{1} of)(a) := \hat{1}(f(a)) := f(a) \Rightarrow \hat{1} of = f,$$

$$(fo\hat{1})(a) := f(\hat{1}(a)) = f(a) \Rightarrow fo\hat{1} = f$$

$$\Rightarrow \forall f \in \Sigma : \quad \hat{1} of = f = fo\hat{1}$$

أى أن Σ مع العمليتين أعلاه هى حلقة

لاحظ أن Σ ليس بالضرورة أن تكون إبدالية ، كما أنها قد تحتوى على قواسم صفرية.

<u>مثال ٦</u> : لتكن R حلقة ، $a, b, c \in R$. يقال أن قانونى الحذف (cancellation laws) متحققان فى R إذا كان

قانون الحذف من جهة اليسار : $a \neq 0, ab = ac \Rightarrow b = c$

قانون الحذف من جهة اليمين : $a \neq 0, ba = ca \Rightarrow b = c$

برهن على أن الحلقة R خالية من القواسم الصفرية إذا كان وفقط إذا كان قانونا الحذف متحققين فى R

<u>البرهان</u> : لتكن R خالية من القواسم الصفرية ولتكن $a, b, c \in R$ وليكن

$$ab = ac, \quad a \neq 0$$

هذا يقتضى أن $a \neq 0 \quad a(b-c)=0,$. ولأن R خالية من القواسم الصفرية ، فإن $a \neq 0$ $b-c=0$ وهذا يؤدى إلى $b=c$. وبالمثل يثبت أن $ba=ca, a \neq 0$ يقتضى أن $b=c$. أى أن قانونى الحذف متحققان .

والآن لنفترض أن قانونى الحذف متحققان فى R والمطلوب إثبات أن R خالية من القواسم الصفرية ليكن $ab=0, a \neq 0 \neq b$. ينتج أن $a\ 0 = a\ b$. ولأن قانون الحذف من جهة اليسار متحقق ينتج أن $b=0$ وهذا تناقض . أى أن R لايمكن أن تحتوى على قواسم صفرية .

<u>**مثال ٧**</u> : ليكن R نظاماً يحقق كل مسلمات (postulates) (أو فروض axioms) الحلقة فيما عدا

$$\forall a,b \in R : a+b=b+a$$

إذا وجد عنصر $c \in R$ بحيث يكون :

$$[\forall a,b \in R : ac=bc \Rightarrow a=b]$$

برهن على أن R حلقة

<u>**البرهان**</u> :

$$\begin{aligned}(a+b)(c+c) &= a(c+c)+b(c+c)\\ &= ac+(ac+bc)+bc \qquad (1)\end{aligned}$$

ولدينا أيضاً

$$\begin{aligned}(a+b)(c+c) &= (a+b)c+(a+b)c\\ &= ac+(bc+ac)+bc \qquad (2)\end{aligned}$$

من (1) ، (2) ينتج أن :

$$ac+bc=bc+ac$$
$$\Rightarrow (a+b)c=(b+a)c$$

وباستخدام خاصة العنصر c ينتج أن

$$a+b=b+a$$

وبالتالى فإن R تكون حلقة .

مثال ٨ : لتكن R حلقة ذات عنصر الوحدة ويتحقق لها $\forall x, y \in R : (xy)^2 = x^2 y^2$

برهن على أن R إبدالية .

البرهان :

$$\forall x, y \in R : [x(y+1)]^2 = x^2 (y+1)^2$$

$$\Rightarrow (xy+x)^2 = x^2 (y^2 + 2y + 1)$$

$$\Rightarrow (xy)^2 + xyx + x^2 y + x^2 = x^2 y^2 + 2x^2 y + x^2$$

$$\Rightarrow xyx = x^2 y \qquad (1)$$

وبالتعويض بــ $x+1$ بدلاً من x نحصل على :

$$(x+1)y(x+1) = (x+1)^2 y$$

$$\Rightarrow (xy+y)(x+1) = (x^2 + 2x + 1)y$$

$$\Rightarrow xyx + xy + yx + y = x^2 y + 2xy + y$$

$$\underset{(1)}{\Rightarrow} xy = yx$$

أى أن R إبدالية .

مثال ٩ : لتكن R حلقة يتحقق لها

$$\forall x \in R : x^3 = x$$

برهن على أن R إبدالية .

البرهان :

$$\forall x, y \in R :$$

$$(x^2 y - x^2 y x^2)^2 = x^2 y . x^2 y - x^2 y x^2 y x^2 - x^2 y x^4 y + x^2 y x^4 y x^2 \qquad (1)$$

ولكن

$$\forall x \in R : x^3 = x \Rightarrow \forall x \in R : x^4 = x^2$$

وبالتعويض فى (1) نحصل على

$$(x^2y-x^2yx^2)^2=x^2yx^2y-x^2yx^2yx^2-x^2yx^2y+x^2yx^2yx^2=0$$

$$\Rightarrow x^2y-x^2yx^2=(x^2y-x^2yx^2)^3=0\Rightarrow x^2y=x^2yx^2 \qquad (2)$$

وبالمثل فلدينا :

$$(yx^2-x^2yx^2)^2=yx^2yx^2-yx^4yx^2-x^2yx^2yx^2+x^2yx^4yx^2 \qquad (3)$$

أيضاً :

$$\forall x\in R: x^4=x^2\Rightarrow (yx^2-x^2yx^2)^2=0$$

$$\Rightarrow yx^2-x^2yx^2=(yx^2-x^2yx^2)^3=0\Rightarrow yx^2=x^2yx^2 \qquad (4)$$

من (2) ، (4) نحصل على :

$$x^2y=yx^2 \qquad (5)$$

أيضاً لدينا :

$$(x^2-x)^3=x^2-x\Rightarrow x^6-3x^5+3x^4-x^3=(x^2)^3-3x^2x^3+3x^2-x$$

$$=x^2-3x^2x+3x^2-x=x^2-3x+3x^2-x=x^2-x$$

$$\Rightarrow -3x+3x^2=0\Rightarrow 3x=3x^2\Rightarrow 2x^2=3x-x^2 \qquad (6)$$

وأيضاً لدينا :

$$\underline{(x^2-x)^2}=x^4-2x^3+x^2=2x^2-2x^3\underset{(6)}{=}3x-x^2-2x^3=3x-x^2-2x=\underline{x-x^2} \qquad (7)$$

ومن (5) لدينا :

$$(x^2-x)^2y=y(x^2-x)^2\underset{(7)}{\Rightarrow}(x-x^2)y=y(x-x^2)\Rightarrow$$

$$xy-x^2y=yx-yx^2\underset{(5)}{\Rightarrow}xy=yx$$

أى أن الحلقة إبدالية .

<u>مثال ١٠</u> : إذا كان كل عنصر فى حلقة R **<u>متماثل القوة</u>** (idempotent) ، أى أن : لكل $x\in R$: $x^2=x$ ، فبرهن على أن R إبدالية . هل العكس صحيح ؟

<u>البرهان</u> : سنبرهن اولاً على أن :

$$\forall x \in R: \quad x+x=0$$

كالآتى :

$$x \in R \Rightarrow x+x \in R \Rightarrow (x+x)^2 = x+x$$

$$\Rightarrow (x+x)(x+x) = x+x \quad \Rightarrow \quad (x+x)x+(x+x)x = x+x$$

قانون التوزيع

$$\Rightarrow \quad (x^2+x^2)+(x^2+x^2) = x+x \underset{x^2=x}{\Rightarrow} (x+x)+(x+x) = x+x$$

قانون التوزيغ

$$\Rightarrow (x+x)+(x+x) = (x+x)+0 \Rightarrow x+x=0 \quad \forall x \in R$$

والآن :

$$a,b \in R \Rightarrow a+b \in R \Rightarrow (a+b)^2 = a+b$$

$$\Rightarrow (a+b)(a+b) = a+b \quad \Rightarrow \quad (a+b)a+(a+b)b = a+b$$

قانون التوزيع

$$\Rightarrow \quad a^2+ba+ab+b^2 = a+b \underset{a^2=a,b^2=b}{\Rightarrow} a+ba+ab+b = a+b$$

قانون التوزيع

$$\Rightarrow ba+ab=0 \Rightarrow ba+ab=ba+ba (\forall x \in R: x+x=0, ba \in R) \Rightarrow ab=ba$$

أى أن R إبدالية .

عكس المقولة ليس صحيحاً بالطبع . مثال مضاد: $\mathbb{R}$ إبدالية ولكن $2^2 \neq 2$ (تسمى هذه الحلقة <u>**حلقة بولية**</u> (Boolean Ring) نسبة إلى الرياضى جورج بول (George Boole) (١٨١٣-١٨٦٤))

<u>مثال ١١</u> : برهن على أنه إذا كان $e \neq 0$ عنصراً متماثل القوة فى نطاق متكامل R فإن e يكون عنصر الوحدة فى R .

<u>البرهان</u> : (حيث 1 هو عنصر الوحدة فى R) $\quad e^2 = e \Rightarrow 0 = ee - e = e(e-1)$

$$\Rightarrow \qquad e-1=0 \Rightarrow e=1$$

$e \neq 0$ و R خال من القواسم الصفرية

مثال ١٢ : يقال لعنصر a فى حلقة أنه **منعدم القوة** (nilpotent) إذا وجد عدد صحيح n أكبر من الصفر بحيث يكون $a^n = 0$. برهن على أن 0 هو العنصر الوحيد منعدم القوة فى أى نطاق متكامل D .

البرهان : ليكن $a \in D$ منعدم القوة . عندئذ فإنه يوجد $n \in \mathbb{N}$: $a^n = 0$ أى أنه يوجد $n \in \mathbb{N}$: $a.a^{n-1} = 0$. ولأن D ليس له قواسم صفرية فإن $a = 0$ أو $a^{n-1} = 0$. إذا كان $a = 0$ نكون قد حصلنا على النتيجة . إذا كان $a^{n-1} = 0$ فبالاستقراء الرياضى يثبت أن $a = 0$.

مثال ١٣ : لتكن R حلقة إبدالية ، وليكن $a, b \in R$ بحيث إن a وحدة ، $b^2 = 0$. برهن على أن $a + b$ وحدة فى R .

البرهان : من حيث إن $a \in R$ وحدة إذن يوجد $R \ni a^{-1}$ بحيث إن $a^{-1}a = 1$ ، 1 هو عنصر الوحدة فى R . والآن :

$$[a^{-1} - (a^{-1})^2 b][a+b] = (a^{-1} - a^{-2}b)(a+b) = a^{-1}a + a^{-1}b - a^{-2}ba - a^{-2}b^2$$

$$= 1 + a^{-1}b - a^{-2}ab - a^{-2}b^2 \qquad \text{(} R \text{ إبدالية)}$$

$$= 1 + a^{-1}b - a^{-1}b - 0 = 1$$

$$= [a+b][a^{-1} - (a^{-1})^2 b] \qquad \text{(} R \text{ إبدالية)}$$

أى أن $a + b$ وحدة فى R .

مثال ١٤ : حدد إذا ما كانت المجموعات الآتية مع عمليات الجمع والضرب الموضحة تعين حلقات :

(أ) $n\mathbb{Z}$ مع عمليتى الجمع والضرب المعتادتين

(ب) $\mathbb{Z}^+$ (مجموعة الأعداد الصحيحة الموجبة)

(جـ) $\mathbb{Z} \otimes \mathbb{Z}$ (الجمع يتم بجمع المركبات ، وكذلك الضرب)

(د) $2\mathbb{Z} \otimes \mathbb{Z}$ الجمع والضرب كما فى (جـ)

(هــ) $\{a+b\sqrt{2} \mid a,b\in \mathbb{Z}\}$ مع عمليتى الجمع والضرب المعتادتين

(و) $\{a+b\sqrt{2} \mid a,b\in \mathbb{Q}\}$ مع عمليتى الجمع والضرب المعتادتين

(ز) مجموعة الأعداد التخيلية الصرفة $r\,i$ حيث $r\in \mathbb{R}$ مع عمليتى الجمع ولضرب المعتادتين

الحل : كل ما سبق يكون حلقاً فيما عدا : المجموعة المعرفة فى (ب) لأن $\mathbb{Z}^{+}$ لاتحتوى على الصفر وهو العنصر المحايد بالنسبة لعملية الجمع (كما أنه لن يكون هناك بالتالى معكوس بالنسبة إلى عملية الجمع) ، المجموعة المعرفة فى (ز) حيث إن حاصل الضرب $ri.si=-rs$ وهذا عدد حقيقى ليس تخيلياً .

مثال ١٥ : فى المثال السابق مباشرة أى الحلقات الواردة تكون إبدالية ؟ لها عنصر الوحدة ؟ حقولاً ؟

الحل :

(أ) إبدالية ، لها عنصر الوحدة إذا كان وفقط إذا كان $n=1$ ، وليست حقلاً لأنه لايوجد معكوس بالنسبة لعملية الضرب لأى عنصر فيما عدا 1 ، -1 (إذا كان $n=1$)

(جـــ) إبدالية : عنصر الوحدة هو $(1, 1)$ ، ليست حقلاً لأنه لايوجد معكوس ضربى أى معكوس بالنسبة لعملية الضرب فيما عدا $(1, 1)$

(د) إبدالية ، ليس لها عنصر الوحدة ، ليست حقلاً

(هــ) إبدالية ، عنصر الوحدة هو $1+0\sqrt{2}$ ، ليست حقلاً لأنه لايوجد معكوس ضربى للعنصر $2+2\sqrt{2}$ مثلاً

(و) إبدالية ، عنصر الوحدة هو $1+0\sqrt{2}$ ، حقل

مثال ١٦ : لتكن $\wp(S)$ تجمع (collection) كل المجموعات الجزئية من S (أو مجموعة القوة لــ S) . سنعرف العمليتين "+" ، "." على $\wp(S)$ كالآتى :-

$$A+B := A\cup B - A\cap B = \{x\in A \text{ or } x\in B \text{ but } x\notin A\cap B\}$$

$$A.B = A\cap B$$

لجمع $A, B \in \wp(S)$

اكتب جدولين لـــ "+" ، "." لـــ $\wp(S)$ حيث $S = \{a, b\}$. وبرهن على أن $(\wp(S), +, .)$ حلقة بولية.

<u>الحل</u> :

.	ϕ	$\{a\}$	$\{b\}$	S
ϕ	ϕ	ϕ	ϕ	ϕ
$\{a\}$	ϕ	$\{a\}$	ϕ	$\{a\}$
$\{b\}$	ϕ	ϕ	$\{b\}$	$\{b\}$
S	ϕ	$\{a\}$	$\{b\}$	S

+	ϕ	$\{a\}$	$\{b\}$	S
ϕ	ϕ	$\{a\}$	$\{b\}$	S
$\{a\}$	$\{a\}$	ϕ	S	$\{b\}$
$\{b\}$	$\{b\}$	S	ϕ	$\{a\}$
S	S	$\{b\}$	$\{a\}$	ϕ

يترك للقارئ البرهنة على أن $(\wp(S), +, .)$ حلقة ومن مثال ١٠ السابق نرى أنها بولية .

<u>مثال ١٧</u> : حدد إذا ما كانت التقريرات الآتية صحيحة أو خاطئة :

(أ) كل حقل يكون حلقة

(ب) كل حلقة لها عنصر الوحدة

(جـ) كل حلقة لها عنصر الوحدة يكون بها وحدتان على الأقل

(د) كل حلقة لها عنصر الوحدة يكون بها وحدتان على الأكثر

(هـ) من الممكن أن تكون هناك مجموعة جزئية من حقل تكون حلقة ، لكنها ليست حقلاً جزئياً .

(و) عملية الضرب فى الحقل إبدالية

(ز) عناصر الحقل غير الصفرية تكون زمرة تحت عملية الضرب فى الحقل

(ح) عملية الجمع فى أية حلقة تكون إبدالية

(ط) كل عنصر فى أية حلقة له معكوس جمعى

<u>الحل</u> : (أ) ، (هـ) ، (و) ، (ز) ، (ح) ، (ط) صحيحة

(ب) ، (جـ) ، (د) خاطئة

أمثلة مضادة : (ب) $2\mathbb{Z}$ حلقة ، ليس لها عنصر الوحدة

(جـ) $\mathbb{Z}_2$ بها وحدة وحيدة وهى عنصر الوحدة $\bar{1}$.

(د) $\mathbb{R}$لها عنصر الوحدة 1 ، كل عناصرها فيما عدا "0" وحدات

سنرى فيما بعد أن $\mathbb{Z}_n, n \in \mathbb{N}$ حلقة وستكون حقلاً إذا كانت n عدداً أولياً .

<u>مثال ١٨</u> : برهن على أن المعكوس الضربى لأى عنصر فى حلقة ذات عنصر الوحدة يكون وحيداً

<u>البرهان</u> : لتكن R حلقة ذات عنصر الوحدة 1 ، وليكن $a \in R$ بحيث إن a^* ، a^{**} معكوسانً لــ a . **والآن :**

$$a^* = 1.a^* = (a^{**}.a).a^* = a^{**}.(a.a^*) = a^{**}.1 = a^{**}$$

<u>مثال ١٩</u> : اضرب مثالاً لعنصرين a ، b فى حلقة بحيث إن $ab = 0$ بينما $ba \neq 0$

<u>الحل</u> : فى حلقة المصفوفات $M_{2\times 2}(\mathbb{Z})$ ليكن $a := \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}$ ، $b := \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}$.

والآن :

$$ab = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$ba = \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

<u>مثال ٢٠</u> : اضرب مثالاً لحلقة غير إبدالية ، وليس لها عنصر الوحدة

<u>الحل</u> : اعتبر $R := \{0, a, b, c\}$ سنعرف الجمع والضرب بالجدولين الآتيين :

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

.	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	a	b	c
c	0	0	0	0

تسمى هذه الجداول جداول كيلى (Cayley's tables)

لاحظ فى هذا المثال أن R لها عنصرا وحدة (ايسران) (أى أنه يوجد r بحيث إن $rx = x$ لجميع $x \in R$) هما a ، b . لكن ليس لها عنصر الوحدة . (الأسهم توضح "اتجاه" الضرب)

<u>**مثال ٢١**</u> : برهن على أن $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ حقل

<u>**البرهان**</u> : البرهان مباشر تماماً . نود فقط ملاحظة أنه لكل عنصر $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ معكوسه الضربى سيكون :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

و $a^2 - 2b^2 \neq 0$ وإلا كان $\sqrt{2} = \dfrac{a}{b}$ وهذا تناقض لأن $\sqrt{2}$ ليس عدداً كسرياً (ليس عدداً نسبياً)

<u>**مثال ٢٢**</u> : اوجد عددين a ، b فى حلقة ، بحيث يكون كل منهما قاسماً صفرياً ، لكن $a + b$ ليس كذلك

<u>**الحل**</u> : فى $\mathbb{Z}_6$: $\bar{2}$ ، $\bar{3}$ قاسمان صفريان لأن $\bar{2} \neq 0 \neq \bar{3}$ ، $\bar{2}.\bar{3} = \bar{0}$ بينما $\bar{5} = \bar{2} + \bar{3}$ ليس قاسماً صفرياً فى $\mathbb{Z}_6$:

$$\bar{5}.\bar{1} = \bar{5} \;,\; \bar{5}.\bar{2} = \bar{4} \;,\; \bar{5}.\bar{3} = \bar{3} \;,\; \bar{5}.\bar{4} = \bar{2} \;,\; \bar{5}.\bar{5} = \bar{1}$$

<u>**مثال ٢٣**</u> : اوجد جميع العناصر فى حلقة R بحيث تكون وحدات ومتماثلة القوة

<u>**الحل**</u> : ليكن u وحدة فى R أى يوجد $v \in R$ بحيث يكون $u\,v = 1$ والآن u متماثلة القوة أى أن $u^2 = u$. ينتج أن $u(uv) = u^2v = uv = 1$ أى أن $u\,1 = 1$ أى أن $u = 1$

<u>**مثال ٢٤**</u> : لتكن R حلقة ذات عنصر الوحدة 1 . إذا كان حاصل ضرب أى عنصرين غير صفريين فيها عنصراً غير صفرى (أى لايساوى الصفر) ، فبرهن على أن :

$$ab = 1 \Rightarrow ba = 1$$

البرهان :

$$\forall a,b \in R \setminus \{0\}:$$

$$ab=1 \Rightarrow aba=a \Rightarrow a(ba-1)=aba-a=0 \underset{a\neq 0}{\Rightarrow} ba=1$$

مثال ٢٥ : ليكن a, b عنصرين فى نطاق متكامل R . برهن على أن :

(أ) $a^5=b^5$ ، $a^3=b^3$ $\Leftarrow$ $a=b$

(ب) $a^m=b^m$ ، $a^n=b^n$ حيث a ، b ليس بينهما قواسم مشتركة (سوى 1 عنصر الوحدة فى R) $\Leftarrow$ $a=b$

البرهان : (أ) $a^3=b^3$ $\Leftarrow$ $a^6=b^6$. والآن :

$$a^6b^5 \underset{a^5=b^5}{=} b^6a^5 \quad = \quad a^5b^6 \underset{a\neq 0\neq b}{\Rightarrow} a=b$$

(قانون الحذف فى النطاق المتكامل) R إبدالى

(الحالة $a=0$ $\Leftarrow$ $b=0$ تافهة)

(ب) m,n ليس بينهما قواسم مشتركة (سوى $1\in R$) وموجبان ، هذا يقتضى وجود عددين صحيحين r, s أحدهما موجب وليكن r والآخر سالب s بحيث يكون $rm+sn=1$

والآن $a^m=b^m$ ، $a^n=b^n$ يستلزم أن :

$$a^{rm}b^{-sn}=b^{rm}a^{-sn} \quad \underset{R\ \text{إبدالى}}{\Rightarrow} \quad a^{rm}b^{-sn}=a^{-sn}b^{rm} \Rightarrow a^{rm+sn}=b^{rm+sn}$$

$$\underset{rm+sn=1}{\Rightarrow} a=b$$

مثال ٢٦ : برهن على أن الحلقة الإبدالية المنتهية R التى ليس لها قواسم صفرية يكون لها عنصر الوحدة

البرهان : لتكن $R:=\{a_1,a_2,...,a_n\}$ ، حيث $a_1\neq 0$. نكون الحلقة $\{a_1a_1,a_1a_2,...,a_1a_n\}$ هذه الحلقة تساوى R لأن كل عناصرها موجودة فى R ، وكذلك إذا كان $a_1a_r=a_1a_s$ ، $r\neq s$ فإن $a_1(a_r-a_s)=0$ ولكن R خالية من القواسم الصفرية ، $a_1\neq 0$ ، وبالتالى فإن $a_r=a_s$ وهذا تناقض . ومن ثم فإن $a_1=a_1a_i$ لبعض i . نبرهن الآن على أن

a_i هو عنصر الوحدة فى R كالآتى: إذا كان $a_k \in R$ فإن: $a_1 a_k = a_1 a_i a_k$ ، ومن ثم فإن $a_1(a_k - a_i a_k) = 0$. مرة أخرى الحلقة ليس لها قواسم صفرية ، $a_1 \neq 0$ وبالتالى فإن $a_i a_k = a_k$. أى أن a_i هو عنصر الوحدة فى R .

<u>**مثال ٢٧**</u> : تعرف رتبة العنصر الجمعية فى الحلقة R برتبته فى الزمرة الجمعية $(R, +)$. لتكن R حلقة إبدالية ليس لها قواسم صفرية . برهن على أن جميع عناصر R غير الصفرية لها نفس الرتبة الجمعية .

<u>**البرهان**</u> : لتكن $a, b \in R \setminus \{0\}$. رتبة a هى m ، رتبة b هى n ، وليكن $m < n$.

والآن : $0 = (ma)b = m(ab) = a(mb) \neq 0$ وهذا تناقض .

(لاحظ أن $a \neq 0$ ، $mb \neq 0$ و R خالية من القواسم الصفرية، وبالتالى فإن$a(mb) \neq 0$) .

<u>**مثال ٢٨**</u> : ليكن D نطاقاً متكاملاً ، ولتكن φ دالة غير ثابتة من D إلى $\mathbb{N}$ بحيث يكون $\varphi(xy) = \varphi(x)\varphi(y)$. برهن على أنه إذا كانت x وحدة فى D فإن $\varphi(x) = 1$.

<u>**البرهان**</u> : $\varphi(x) = \varphi(1.x) = \varphi(1)\varphi(x)$ ، وبالتالى فإن $\varphi(1) = 1$ (قانون الحذف فى النطاق المتكامل) .

والآن : $\varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x)$ $\underset{x \text{ وحدة}}{=}$ $1 = \varphi(1)$ وبالتالى فإن $\varphi(x) \neq 0$

ولأن "صور" φ دائماً أعداد صحيحة موجبة فإن $\varphi(x) = 1$

تمارين

(١) برهن على أن مجموعة الدوال الحقيقية المتصلة التى يمر رسمها بالنقطة (1, 0) تكون حلقة إبدالية ، ليس لها عنصر الوحدة مع العمليتين :

$$\forall a \in \mathbb{R} : (f+g)(a) := f(a)+g(a), (f.g)(a) := f(a).g(a)$$

(٢) لتكن R_1 ، ... ، R_n حلقات . سنكون :

$$R := R_1 \otimes R_2 \otimes \ldots \otimes R_n := \{(a_1, a_2, \ldots, a_n) \mid a_i \in R_i\}$$

ونعرف الجمع والضرب كالآتى :

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) := (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

$$(a_1, a_2, \ldots, a_n).(b_1, b_2, \ldots, b_n) := (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

برهن على أن هذا التكوين مع هاتين العمليتين يمثل حلقة (تسمى **حاصل الضرب المباشر** للحلقات R_1 ، R_2 ، ... ، R_n ، سندرسها فيما بعد) .

(٣) فى التمرين السابق مباشرة لتكن R_1 ، R_2 ، ... ، R_n تحتوى على عناصر غير صفرية . برهن على أن R لها عنصر وحدة إذا كان وفقط إذا كان كل R_i تحتوى على عنصر وحدة .

(٤) اعط مثالاً لحلقة غير منتهية ، غير إبدالية ، ليس لها عنصر وحدة

(٥) برهن على أن $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ حلقة مع عمليتى الجمع والضرب المعتادتين للأعداد الحقيقية .

(٦) برهن على أن الحلقة التى تكون دائرية تحت عملية الجمع تكون إبدالية

(٧) عين $U(\mathbb{Z}[X])$ ، $U(\mathbb{R}[X])$ ($U(R)$ هى مجموعة كل الوحدات فى R)

(٨) فى $\mathbb{Z}_6$ برهن على أن $\bar{4} \mid \bar{2}$ ؛ فى $\mathbb{Z}_8 : \bar{3} \mid \bar{7}$ ؛ وفى $\mathbb{Z}_{15} : \bar{9} \mid \overline{12}$

(٩) اوجد عدداً صحيحاً n يظهر أن الحلقة $\mathbb{Z}_n$ لاتحقق بالضرورة الخصائص الآتية للحلقة $\mathbb{Z}$:

(أ) $a^2 = a$ يستلزم أن $a = \bar{0}$ أو $a = \bar{1}$

(ب) $ab = \bar{0}$ يستلزم أن $a = \bar{0}$ أو $b = \bar{0}$

(جـ) $a\,b = a\,c$ يستلزم $b = c$

هل n التى حصلت عليها عدد أولى ؟

(١٠) برهن على أن أى وحدة فى حلقة تقسم كل عنصر فى الحلقة

(١١) فى مثال ٢٠ السابق برهن على أنه يوجد عنصرا وحدة أيسران ، (أى أنه يوجد r بحيث يكون $rx = x$ لجميع x فى الحلقة) بينما لايوجد عنصر وحدة أيمن

(١٢) المجموعة $\{\overline{0}, \overline{2}, \overline{4}\}$ تحت عمليتى الجمع والضرب مقياس 6 تكون حلقة إبدالية ذات عنصر وحدة . برهن على ذلك

(١٣) فى حلقة ما يتحقق $x^3 = x$ لجميع x . برهن على أن $a\,b = 0$ يستلزم $b\,a = 0$

(١٤) برهن على أن أية وحدة فى حلقة ذات عنصر وحدة يكون معكوسها الضربى وحيداً

(١٥) اعتبر $(S, +, .)$ ، حيث S مجموعة ، "+" ، "." عمليتان على S بحيث إن :

(أ) $(S, +)$ زمرة

(ب) $(S^*, .)$ زمرة حيث S^* تتكون من جميع عناصر S ماعدا عنصرها المحايد بالنسبة إلى "الجمع" أى الصفر

(جـ) $a(b + c) = a\,b + a\,c$

$(a + b)\,c = a\,c + b\,c$

لجميع $a, b, c \in S$

برهن على أن $(S, +, .)$ شبه حقل .

(إرشاد : استخدم قوانين التوزيع على $(1 + 1)(a + b)$ لكى تبرهن على أن عملية "الجمع" إبدالية).

(١٦) لتكن R حلقة ، $a, b, c \in R$ برهن على أن :

$$a(b - c) = ab - ac, (b - c)a = ba - ca$$

وإذا كان $1 \in R$ (عنصر الوحدة) فإن

$$(-1)\,a = -\,a \quad , \quad (-1)\,(-1) = 1$$

(١٧) إذا كان $m, n \in \mathbb{Z}$ ، R حلقة ، $a, b \in R$ فبرهن على أن : $(ma)(nb) = (mn)(ab)$

(١٨) إذا كان $n\in\mathbb{Z}$ ، R حلقة ، $a\in R$ فبرهن على أن : $n(-a)=-(na)$

(١٩) لتكن R حلقة، $a,b\in R$، $m\in\mathbb{Z}$. فبرهن على أن: $m(ab)=(ma)b=a(mb)$

(٢٠) لتكن R حلقة . برهن على أن R إبدالية إذا كان وفقط إذا كان :

$$\forall a,b\in R:\quad a^2-b^2=(a+b)(a-b)$$

(٢١) لتكن R حلقة ويوجد عدد زوجى موجب n لكل $a\in R$ بحيث يكون $a^n=a$. برهن على أنه لكل $a\in R$ يكون : $-a=a$.

(٢٢) ما وجه (أو أوجه) الخطأ فى البرهان الآتى على أن $(-a)(-b)=ab$:

$$(-a)(-b)=(-1)a(-1)b=(-1)(-1)ab=1ab=ab$$

(٢٣) اوجد حلول المعادلة $x^3-2x^2-3x=0$ فى $\mathbb{Z}_{12}$

(٢٤) حل المعادلة $3x=2$ فى $\mathbb{Z}_7$ ، $\mathbb{Z}_{23}$

(٢٥) حل المعادلة $x^2+2x+2=0$ فى $\mathbb{Z}_6$

(٢٦) حل المعادلة $x^2+2x+4=0$ فى $\mathbb{Z}_6$

(٢٧) حدد إذا ما كانت التقريرات الآتية صحيحة أم خاطئة :

(أ) $n\mathbb{Z}$ لها قواسم صفرية إذا كانت n ليست عدداً أولياً .

(ب) كل حقل يكون نطاقاً متكاملاً .

(جـ) أى قاسم صفرى فى حلقة إبدالية ذات عنصر الوحدة لايكون له معكوس ضربى

(د) $M_{n\times n}(F)$ حيث F هو $\mathbb{Q}$ أو $\mathbb{R}$ أو $\mathbb{C}$ ، ليس لها قواسم صفرية لأى n

(هـ) كل عنصر غير صفرى من $M_{2\times2}(\mathbb{Z}_2)$ يكون وحدة

(و) الحلقة $\mathbb{Z}_n$ (حلقة الأعداد الصحيحة مقياس n) نطاق متكامل

(ز) الحلقة $M_{2\times2}(\mathbb{Z})$ (حلقة المصفوفات المربعة من النوع 2×2 ومداخلها (عناصرها) أعداد صحيحة) نطاق متكامل

(ح) $\mathbb{Z}_3[i]=\{a+bi\mid a,b\in\mathbb{Z}_3\}$ حقل مكون من تسعة عناصر

(٢٨) أى المجموعات الآتية تكون حقلاً ؟

(أ) $\mathbb{Z}$ (ب) $\mathbb{Z}[i] := \{a+bi \mid a,b \in \mathbb{Z}\}$

(جـ) $\mathbb{Z}[X]$ (د) $\mathbb{Z}[\sqrt{2}] := \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$

(هـ) $\mathbb{Z}_p$ (حلقة الأعداد الصحيحة مقياس العدد الأولى p)

(٢٩) برهن على أن أية حلقة إبدالية يتحقق لها قانونا الحذف (انظر مثال ٦ فى (١-١-١٥)) تكون خالية من القواسم الصفرية

(٣٠)اضرب مثالاً لحلقة إبدالية تكون خالية من القواسم الصفرية ، لكنها ليست نطاقاً متكاملاً

(٣١) ليكن a عنصراً فى حلقة R لها عنصر الوحدة 1 ، وليكن $a^n = 0$ ، حيث n عدد صحيح موجب (يسمى a عنصراً منعدم القوة ، كما ورد فى مثال ١٢ من (١-١-١٥))

برهن على أن $1-a$ له معكوس ضربى .

(إرشاد : اعتبر $((1-a)(1+a+a^2+...+a^{n-1})$)

(٣٢) برهن على أن 0 ، 1 هما العنصران الوحيدان متماثلا القوة فى أى نطاق متكامل (انظر مثال ١٠ فى (١-١-١٥))

(٣٣) برهن على أن حاصل ضرب عنصرين متماثلى القوة فى حلقة ما هو عنصر متماثل القوة فى الحلقة

(٣٤) ليكن d عدداً صحيحاً موجباً ليس مربعاً . برهن على أن :

$$\mathbb{Q}[\sqrt{d}] := \{a+b\sqrt{d} \mid a,b \in \mathbb{Q}\}$$ حقل

(٣٥) ليكن $R = \{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\}$ تحت عمليتى الجمع والضرب مقياس 10 . برهن على أن R حقل

(٣٦) كيف تعرف النطاق المتكامل الجزئى ؟

ليكن D نطاقاً متكاملاً له عنصر الوحدة1 . برهن على أن $P := \{n1 \mid n \in \mathbb{Z}\}$ يكون نطاقاً متكاملاً جزئياً من D . برهن كذلك على أن P يكون محتوى فى كل نطاق متكامل جزئى من D .

(إرشاد : النطاق المتكامل الجزئى S من النطاق المتكامل D هو مجموعة جزئية من D بحيث إن عمليتى الجمع والضرب على D محددتين على S تجعلان S نطاقاً متكاملاً . للبرهنة على أن P نطاق جزئىٌ من D نبرهن على أنه لكل $a,b\in P$: $a-b\in P$ ، $a.b\in P$ ، $1\in P$. كل نطاق جزئى من D يحتوى على 1 ، ويحتوى على $n1$ حيث $n\in\mathbb{Z}$ ، وبهذا يحتوى على P).

(٣٧) برهن على أنه لايوجد نطاق متكامل يتكون من ستة عناصر . ماذا عما إذا كان يتكون من أربعة عناصر ، خمسة عشر عنصراً ؟

(إرشاد : تذكر أن كل نطاق متكامل منته يكون حقلاً !)

(٣٨) عين كل عناصر النطاق المتكامل التى تكون هى معكوسات نفسها

(٣٩) عين حقلاً منتهياً يكون فيه عنصران غير صفريين a ، b بحيث إن $a^2+b^2=0$

(٤٠) أنشئ جدول الضرب لــ $\mathbb{Z}_2[i]$. $(\mathbb{Z}_2[i]:=\{a+bi\mid a,b\in\mathbb{Z}_2)$

هل هذه الحلقة حقل ؟ هل هى نطاق متكامل ؟

(٤١) لتكن R حلقة إبدالية ، $a,b\in R$ بحيث إن ab قاسم صفرى فى R . برهن على أن a قاسم صفرى فى R أو b قاسم صفرى فى R .

(٤٢) حل المعادلة $x^2-x+2=0$ فى $\mathbb{Z}_3[i]$

(٤٣) اعتبر المعادلة $x^2-5x+6=0$

(أ) كم عدد حلول المعادلة فى $\mathbb{Z}_7$ ؟

(ب) اوجد جميع الحلول فى $\mathbb{Z}_8$

(جـ) اوجد جميع الحلول فى $\mathbb{Z}_{12}$

(د) اوجد جميع الحلول فى $\mathbb{Z}_{14}$

(٤٤) ليكن F حقلاً منتهياً ، ذا n من العناصر . برهن على أن $x^{n-1}=1$ لجميع العناصر غير الصفرية فى F .

(٤٥) وضح لماذا لايمكن لحلقة إبدالية ذات عنصر الوحدة لكنها ليست نطاقاً متكاملاً أن تكون محتواة فى حقل

(٤٦) اضرب مثالاً لحلقة ليس لها عنصر الوحدة تكون محتواة فى حق

٢-١ هومومورفيزم الحلق ، الحلقة الجزئية والمثالى

Ring homomorphisms, Subrings and Ideals

١-٢-١ تعريف : لتكن $(R, +, .)$ ، $(R',+',.')$ حلقتين . يسمى الراسم $\varphi: R \to R'$ **هومومورفيزم حلق** (ring homomorphism) إذا تحقق : لكل $a,b\in R$:

(أ) $\varphi(a+b)=\varphi(a)+'\varphi(b)$

(ب) $\varphi(a.b)=\varphi(a).'\varphi(b)$

بعض المراجع يضع شرطاً ثالثاً وهو :

(جـ) إذا كان $1\in R$ ، $1'\in R'$ عنصرى الوحدة فإن $\varphi(1)=1'$

المفاهيم: **مونومورفيزم**(monomorphism)، **إبيمورفيزم**(epimorphism) ، **أيزومورفيزم** (isomorphism)، **إندومورفيزم** (endomorphism) ، **أوتومورفيزم**(automorphism) . تعرف مناظرة لنفسها فى نظرية الزمر . وللسهولة فى الكتابة لن نضع غالباً "." ، "'." وسنكتب "+" وليس " '+ ".

ليكن $\varphi:R\to R'$ هومومورفيزم حلقياً . نعرف المجموعة $Ker(\varphi):=\{a\in R|\varphi(a)=0'\}$ ($0'$ صفر الحلقة R') بأنها نواة (φ) (Kernel (φ))

١-٢-٢ ملحوظات : ليكن $\varphi: R \to R'$ هومومورفيزم حلق

(أ) φ راسم أحادى $\Leftrightarrow$ $Ker(\varphi)=\{0\}$ (0 هو صفر الحلقة R)

(ب) φ أيزومورفيزم حلقى $\Leftrightarrow$ φ^{-1} أيزومورفيزم حلقى

(جـ) $\psi: R'\to R''$ هومومورفيزم حلق $\Leftarrow$ $\psi o\varphi: R\to R''$ هومومورفيزم حلق

البرهان : مشابه لما جاء فى نظرية الزمر

١-٢-٣ تعريف : لتكن $\phi\neq S\subset R$ حيث R حلقة . تسمى S **حلقة جزئية** (subring) من R إذا تحقق :

(أ) $\forall a,b:\ \ a,b\in S\Rightarrow[a+b\in S,\ \ ab\in S]$

(ب) S مع العمليتين المستحدثتين $S\times S\to S,(a,b)\mapsto a+b$ ، $S\times S\to S,(a,b)\mapsto ab$ تكون حلقة .

١-٢-٤ ملحوظة : لتكن R حلقة ، $\phi\neq S\subset R$. التقريرات الآتية متكافئة .

(أ) S حلقة جزئية من R

(ب) S زمرة جزئية من الزمرة الجمعية لـــ R ، $a,b\in S\Rightarrow ab\in S$

(جـ) $ab\in S \quad , \quad a,b\in S\Rightarrow a-b\in S$

البرهان : مباشر وراجع (١-٤-١) ، (١-٤-٢) فى نظرية الزمر .

١-٢-٥ تعريف : ليكن حلقة $\phi\neq A\subset R$. A **مثالى** (ideal) إذا تحقق :

(أ) A زمرة جزئية من الزمرة الجمعية لـــ R

(ب) $\forall a\in A \;\; \forall b\in R\Rightarrow ba\in A, ab\in A$

١-٢-٦ ملحوظة : R حلقة ، $\phi\neq A\subset R$. التقريران الآتيان متكافئان

(أ) A مثالى فى R

(ب) $\forall a,b\in A: \quad a-b\in A,$

$\forall r\in R \quad \forall a\in A: ra\in A, ar\in A$

١-٢-٧ أمثلة :

(١) كل حلقة R تحتوى على حلقتين جزئيتين تافهتين هما $\{0\}$ ، R (حيث 0 هو العنصر الصفرى فى R أى صفر الحلقة R) . هما كذلك المثاليان التافهان لأى حلقة R . أى مثالى غير تافه يقال له **مثالى فعلى** (proper ideal) ، وأى حلقة جزئية غير تافهة يقال إنها **حلقة جزئية فعلية** (proper subring)

(٢) لتكن R حلقة إبدالية . عندئذ فإنه لأى $a\in R$ تكون المجموعة

$Ra:=\{ra\mid r\in R\}$

مثاليا فى R

البرهان : $Ra\neq\phi$: لأن (١) $0=0a\in Ra$

كذلك : (٢) لجميع $ra, sa \in Ra$:

$$ra - sa = (r-s)a \in Ra$$

و (٣) لجميع $ra \in Ra$ ، $s \in R$:

$$s(ra) = (sr)a \in Ra,$$

$$(ra)s \quad = \quad s(ra) = (sr)a \in Ra$$

R إبدالية

من (١) ، (٢) ، (٣) ينتج الادعاء مباشرة .

(٣) $\phi \neq A \subset \mathbb{Z}$. A مثالى فى $\mathbb{Z}$ $\Leftrightarrow$ $\exists m \in \mathbb{N} : A = m\mathbb{Z}$

<u>البرهان</u> : من مثال ٣ فى (١-٤-٤) من نظرية الزمر ، ومن (١-٢-٦) أعلاه يكفى أن نبرهن على أن :

$$\forall n \in \mathbb{Z} \ \ \forall a \in A : na \in A, an \in A \qquad\qquad (*)$$

والآن فإنه لكل $a \in A$ يوجد $z \in \mathbb{Z}$ بحيث إن $a = mz$.

$$\forall n \in \mathbb{Z} \quad \forall mz \in A: \ \ n(mz) = m(nz) \in m\mathbb{Z} = A,$$

$$(mz)n = m(zn) \in m\mathbb{Z} = A.$$

وبدهى أنه إذا لم يتحقق (*) فإن A لن يكون مثالياً .

(٤) $\{\bar{0}, \bar{2}, \bar{4}\}$ حلقة جزئية من ($\mathbb{Z}_6 := \{\bar{0}, \bar{1}, ..., \bar{5}\}$)

(٥) $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ حلقة جزئية من الحلقة (الحقل) $\mathbb{C}$ لكنها ليست مثالياً فى $\mathbb{C}$.

(٦) كل مثالى هو حلقة جزئية ، لكن ليست كل حلقة جزئية مثاليا (مثال مضاد : مثال (٥) السابق مباشرة)

<u>١-٢-٨ أمثلة متنوعة</u> :

<u>مثال ١</u> : لتكن R حلقة ، وليكن $a \in R$. برهن على أن $S := \{x \in R \mid ax = 0\}$ حلقة جزئية من R

<u>البرهان</u> : $0 \in R$ ، $a0 = 0$ يقتضى أن $0 \in S$ ، أى أن $S \neq \phi$.

كذلك فليكن $x, y \in S$ هذا يقتضى أن : $ax = 0$ ، $ay = 0$. والآن :

$$a(x-y) = ax - ay = 0 - 0 = 0 \Rightarrow x - y \in S$$

كذلك فإن :

$$a(xy) = (ax)y = 0y = 0$$

أى أن $xy \in S$. ومن ثم البرهان .

__مثال ٢__ : لتكن R حلقة . يعرف __مركز__ (The centre of R) $\underline{\boldsymbol{R}}$ بأنه المجموعة $S := \{x \in R \mid ax = xa \ \forall a \in R\}$. برهن على أن مركز R حلقة جزئية من R .

__البرهان__ : من مثال ٤٩ من أمثلة متنوعة على نظرية الزمر ، ومن (١-٢-٤) أعلاه يكفى أن نبرهن على أن

$$\forall x, y: \quad x, y \in S \Rightarrow xy \in S$$

$$x, y \in S \Rightarrow ax = xa \quad \forall a \in R \qquad (1),$$

$$ay = ya \quad \forall a \in R \qquad (2)$$

والآن :

$$\forall a \in R: \quad a(xy) = (ax)y \underset{(1)}{=} (xa)y = x(ay) \underset{(2)}{=} x(ya) = (xy)a$$

أى أن : $\forall\, x, y \in S : xy \in S$

__مثال ٣__ : لتكن $1 \in R$ حلقة (أى لها عنصر الوحدة) ، $a \in R$ بحيث إن $a^2 = 1$.

برهن على أن $S := \{ara \mid r \in R\}$ حلقة جزئية من R . هل $1 \in S$ ؟

__البرهان__ : $1 = a^2 = aa \underset{1 \in R}{=} a1a \in S$ ، أى أن $S \neq \phi$.

$$ara, asa \in S \Rightarrow ara - asa = a(r-s)a \underset{r-s \in R}{\in} S,$$

$$araasa = ara^2sa = ar1sa = arsa \underset{rs \in R}{\in} S$$

ومن ثم فإن S حلقة جزئية من R وتحتوى على عنصر الوحدة 1 .

<u>مثال ٤</u> : لتكن $R:=\left\{\begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \mid a,b\in\mathbb{Z}\right\}$. برهن أو انف : R حلقة جزئية من $M_{2\times2}(\mathbb{Z})$.

<u>الحل</u> :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\in R \text{ أى أن } R\neq\phi$$

والآن ليكن $\begin{pmatrix} a & a-b \\ a-b & b \end{pmatrix}\in R$ ، $\begin{pmatrix} c & c-d \\ c-d & d \end{pmatrix}$ حيث $a,b,c,d\in\mathbb{Z}$:

$$\begin{pmatrix} a & a-b \\ a-b & b \end{pmatrix}-\begin{pmatrix} c & c-d \\ c-d & d \end{pmatrix}=\begin{pmatrix} a-c & a-c-(b-d) \\ a-c-(b-d) & b-d \end{pmatrix}\in R$$

$$\begin{pmatrix} a & a-b \\ a-b & b \end{pmatrix}\cdot\begin{pmatrix} c & c-d \\ c-d & d \end{pmatrix}=\begin{pmatrix} 2ac-ad-bc+bd & ac-bd \\ ac-bd & ac-ad-bc+2bd \end{pmatrix}\in R$$

أى أن R حلقة جزئية من $M_{2\times2}(\mathbb{Z})$.

<u>مثال ٥</u> : برهن على أن $2\mathbb{Z}\cup3\mathbb{Z}$ ليست حلقة جزئية من $\mathbb{Z}$

<u>البرهان</u> : $2\in2\mathbb{Z}$ ، $3\in3\mathbb{Z}$ ، لكن $3-2=1\notin2\mathbb{Z}\cup3\mathbb{Z}$

<u>مثال ٦</u> : لتكن $R:=\mathbb{R}\otimes\mathbb{R}\otimes\mathbb{R}$ كما فى (٢) من التمارين على (١-١) ،

$S:=\{(a,b,c)\in R \mid a+b=c^2\}$

برهن أو انف : S حلقة جزئية من R . (تحقق من أن R حلقة !)

<u>الحل</u> : $(0,1,1),(2,2,2)\in S$ بينما $(2,2,2)-(0,1,1)=(2,1,1)\notin S$

وبالتالى فإن S ليس حلقة جزئية من R .

<u>مثال ٧</u> : اوجد أصغر حلقة جزئية من $\mathbb{Q}$ تحتوى على $\frac{1}{2}$

<u>الحل</u> : نبرهن على أن $S=\{\frac{m}{2^n}\mid m\in\mathbb{Z},n\in\mathbb{N}\}$ هى الحلقة الجزئية المطلوبة

واضح أن S حلقة جزئية من $\mathbb{Q}$

لأن $S \in \frac{0}{2^n} = 0$ أى أن S غير خالية

$$\Leftarrow \frac{m_1}{2^{n_1}}, \frac{m_2}{2^{n_2}} \in S$$

$$\frac{m_1}{2^{n_1}} - \frac{m_2}{2^{n_2}} = \frac{m_3}{2^{n_3}}, m_3 \in \mathbb{Z}, n_3 \in \mathbb{N} \ .$$

$$\frac{m_1}{2^{n_1}} \frac{m_2}{2^{n_2}} = \frac{m_1 m_2}{2^{n_1+n_2}} \in S$$

والآن أية حلقة جزئية من $\mathbb{Q}$ تحتوى على $\frac{1}{2}$ لابد أن تحتوى على $\left(\frac{1}{2}\right)^n$ حيث $n \in \mathbb{N}$ ،

وكذلك تحتوى على $\pm \frac{r}{2} = \pm\left(\frac{1}{2}+...+\frac{1}{2}\right)$ وبالتالى فهى تحتوى على كل العناصر $\frac{m}{2^n}$

حيث $m \in \mathbb{Z}$ ، $n \in \mathbb{N}$. ومن ثم البرهان .

<u>مثال ٨</u> : لتكن R حلقة . برهن على أنه لجميع $a,b \in R$ يكون $a^2-b^2=(a-b)(a+b)$

إذا كانت وفقط إذا كانت R حلقة إبدالية .

<u>البرهان</u> : $\forall a,b \in R : (a-b)(a+b) = a^2 + ab - ba - b^2$

إذا كانت R إبدالية فإن $ab = ba$ وبالتالى فإن :

$$(a-b)(a+b) = a^2 - b^2$$

وبالعكس إذا كان $(a-b)(a+b) = a^2 - b^2$ فإن $ab - ba = 0$ ويكون $ab = ba$ أى أن

R إبدالية . (انظر (٢٠) فى تمارين (١-١) (!)) .

<u>مثال ٩</u> : ليكن $\varphi : R \to S$ هومومورفيزم حلق . برهن على أن :

$$\forall r \in R \quad \forall n \in \mathbb{N} : \quad \varphi(nr) = n\varphi(r)$$

$$\varphi(r^n) = \varphi(r)^n$$

البرهان : بالاستقراء الرياضى : عند $n = 1$ واضح أن التقريرين صحيحان :

عند $n = m + 1$:

$$\varphi((m+1)r) = \varphi(mr + r) = \varphi(mr) + \varphi(r)$$

$$= m\varphi(r) + \varphi(r) = (m+1)\varphi(r),$$

فرض الاستقراء

$$\varphi(r^{m+1}) = \varphi(rr^m) = \varphi(r)\varphi(r^m) = \varphi(r)\varphi(r)^m = \varphi(r)^{m+1}$$

فرض الاستقراء

<u>مثال ١٠</u> : ليكن $\varphi : R \to S$ هومومورفيزم حلق . وليكن 1 عنصر الوحدة فى R ، $S \neq \{0\}$ ، وكان φ راسماً غامراً (شاملاً ، فوقياً) ، عندئذ فإن $\varphi(1)$ يكون عنصر الوحدة فى S .

<u>البرهان</u> : φ غامر يقتضى أنه لكل $y \in S$ يوجد $x \in R$ بحيث إن $\varphi(x)=y$. والآن :

$$\varphi(1)y = \varphi(1)\varphi(x) = \varphi(1x) = \varphi(x) = y,$$

$$y\varphi(1) = \varphi(x)\varphi(1) = \varphi(x1) = \varphi(x) = y$$

وينتج المطلوب مباشرة .

<u>مثال ١١</u> : ليكن $\varphi : R \to S$ هومومورفيزم حلق . وليكن $A \subset R$ مثاليا ، $B \subset R$ حلقة جزئية ، $A' \subset S$ مثاليا ، $B' \subset S$ حلقة جزئية .

برهن على أن :

(أ) φ غامر (شامل) $\Leftarrow$ $\varphi(A) \subset S$ مثالى

(ب) $\varphi^{-1}(A') \subset R$ مثالى

(جـ) $\varphi(B) \subset S$ حلقة جزئية

(د) $\varphi^{-1}(B') \subset R$ حلقة جزئية

<u>البرهان</u> : (أ) من ملحوظة (١-٤-٣ (أ)) فى نظرية الزمر ، ومن (١-٢-٥) أعلاه يكفى أن نبرهن على أنه :

$$\forall \varphi(a) \in \varphi(A) \quad \forall s \in S : s\varphi(a) \in \varphi(A), \varphi(a)s \in \varphi(A)$$

ومن حيث إن φ غامر فإنه لكل $s \in S$ يوجد $r \in R$ بحيث يكون $\varphi(r) = s$ ولدينا :

$$s\varphi(a) = \varphi(r)\varphi(a) = \varphi(ra) \underset{\text{مثالى } A \subset R}{\in} \varphi(A), \varphi(a)s = \varphi(a)\varphi(r) = \varphi(ar) \underset{\text{مثالى } A \subset R}{\in} \varphi(A)$$

(ب) من ملحوظة (١-٤-٣ (ب)) فى نظرية الزمر ومن (١-٢-٥) أعلاه يكفى أن نبرهن على أنه :

$$\forall a \in \varphi^{-1}(A') \ \ \forall r \in R : ra \in \varphi^{-1}(A'), ar \in \varphi^{-1}(A')$$

والآن :

$$a \in \varphi^{-1}(A') \Rightarrow \varphi(a) \in A' \Rightarrow \varphi(ra) = \varphi(r)\varphi(a) \underset{\text{مثالى } A' \subset S}{\in} A'$$

$$\Rightarrow ra \in \varphi^{-1}(A')$$

وبالمثل $ar \in \varphi^{-1}(A')$

(جـ) من ملحوظة (١-٤-٣ (أ)) فى نظرية الزمر ومن (١-٢-٤) أعلاه يكفى أن نبرهن على أنه :

$$\forall x', y' \in \varphi(B) : x'y' \in \varphi(B)$$

والآن :

$$x', y' \in \varphi(B) \Rightarrow \exists x, y \in B : x' = \varphi(x), y' = \varphi(y) \Rightarrow \varphi(xy)$$
$$= \varphi(x)\varphi(y) = x'y' \ .$$

ومن حيث إن B حلقة جزئية فى R فإن $xy \in B$ وبالتالى فإن $\varphi(xy) \in \varphi(B)$ أى أن $x'y' \in \varphi(B)$

(د) من ملحوظة (١-٤-٣ (ب)) فى نظرية الزمر ، ومن (١-٢-٤) أعلاه يكفى أن نبرهن على أن:

$$\forall x, y \in \varphi^{-1}(B') : xy \in \varphi^{-1}(B')$$

والآن :

$$x,y \in \varphi^{-1}(B') \Rightarrow \varphi(x),\varphi(y) \in B' \Rightarrow \varphi(xy) = \varphi(x)\varphi(y) \quad \in \quad B'$$

B' حلقة جزئية فى S

$$\Rightarrow xy \in \varphi^{-1}(B'),$$

<u>مثال ١٢</u> : ليكن $\varphi: R \to S$ هومومورفيزم حلق . برهن على أنه إذا كانت R حلقة إبدالية فإن $\varphi(R)$ تكون حلقة جزئية إبدالية فى S .

<u>البرهان</u> : من حيث إن R حلقة جزئية من نفسها فإنه من مثال ١١ (جـ) السابق مباشرة تكون $\varphi(R)$ حلقة جزئية من S . والآن

$$\forall x', y' \in \varphi(R) \;\; \exists x, y \in R : x' = \varphi(x), y' = \varphi(y).$$

$$x'y' = \varphi(x)\varphi(y) = \varphi(xy) \underset{R \text{ إبدالية}}{=} \varphi(yx) = \varphi(y)\varphi(x) = y'x'$$

وينتج المطلوب مباشرة .

<u>مثال ١٣</u> : برهن أو انف : (أ) الحلقة $2\mathbb{Z}$ تتشاكل (أيزومورفية) مع الحلقة $3\mathbb{Z}$

(ب) الحلقة $2\mathbb{Z}$ تتشاكل مع الحلقة $4\mathbb{Z}$

<u>الحــل</u> : ليكن $\begin{array}{c}\varphi: 2\mathbb{Z} \to 3\mathbb{Z} \\ 2x \mapsto 3x\end{array}$ أيزومورفيزم حلق .

والآن :

$$\varphi(2.2) = 3.2 = 6 \neq 9 = 3.3 = \varphi(2)\varphi(2)$$

التقرير خاطئ . (لاحظ أن 2 مولد لـــ $2\mathbb{Z}$ ، 3 مولد لـــ $3\mathbb{Z}$)

(ب) بالمثل وأكمل ...

<u>مثال ١٤</u> : برهن أو انف : الحقلان $\mathbb{R}$ ، $\mathbb{C}$ متشاكلان $(\mathbb{R} \cong \mathbb{C})$

<u>الحــل</u> : التقرير خاطئ . المعادلة $x^2 = -1$ لها حلان فى $\mathbb{C}$ هما $i, -i$ بينما ليس لها حـــل فى الحقل $\mathbb{R}$

<u>مناقشة أخرى</u> : إذا كان $\mathbb{R}$ ، $\mathbb{C}$ متشاكلين فإن $\mathbb{R} \setminus \{0\}$ ، $\mathbb{C} \setminus \{0\}$ يكونان متشاكلين كذلك . لكن كل عنصر فى $\mathbb{R} \setminus \{0\}$ يولد زمرة دائرية غير منتهية فيما عدا العنصرين

1، 1- فإنهما يولدان زمرتين دائريتين لهما الرتبة 1 ، 2 على الترتيب . أما فى $\mathbb{C}\setminus\{0\}$ فإن العنصر i يولد الزمرة الدائرية $\{i,-1,-i,1\}$ ذات الرتبة 4 . (العملية فى الحالتين هى الضرب المعتاد)

مثال ١٥ : ليكن
$$\varphi : M_{2\times2}(\mathbb{Z}) \to \mathbb{Z}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$$
برهن أو انف : φ هومومورفيزم حلق

الحل :

$$\varphi\left(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\right) = \varphi\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = 2 \neq 1 = 1.1 = \varphi\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\varphi\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

أى أن φ ليس هومومورفيزم حلق .

مثال ١٦ : لتكن $R := \left\{\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a,b,c \in \mathbb{Z}\right\}$. برهن أو انف :

$$\varphi : R \to \mathbb{Z}$$
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$$

هومومورفيزم حلق .

الحــل :

$$\forall \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in R :$$

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right) = \varphi\begin{pmatrix} a+x & b+y \\ 0 & c+z \end{pmatrix} = a+x = \varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \varphi\begin{pmatrix} x & y \\ 0 & z \end{pmatrix},$$

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right) = \varphi\begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix} = ax = \varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\varphi\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$$

أى أن φ هومومورفيزم حلق .

(يترك للقارئ التحقق من R حلقة ، وهى حلقة جزئية من $(M_{2\times2}(\mathbb{Z})$.

مثال ١٧ : لتكن $\mathbb{Z}[\sqrt{2}] := \{a+b\sqrt{2} \mid a,b\in \mathbb{Z}\}$. (تحقق من أن $\mathbb{Z}[\sqrt{2}]$ حلقة) .

لتكن

$$H := \left\{\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a,b\in \mathbb{Z}\right\}$$

تحقق كذلك من أن H حلقة جزئية من $M_{2\times2}(\mathbb{Z})$. برهن على أن $\mathbb{Z}[\sqrt{2}]$ ، H متشاكلتان

البرهان : $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\in H$ أى أن H غير خالية . والآن ليكن $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix},\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}\in H$:

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}-\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}=\begin{bmatrix} a-c & 2(b-d) \\ b-d & a-c \end{bmatrix}\in H$$

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}=\begin{bmatrix} ac+2bd & 2(ad+bc) \\ ad+bc & ac+2bd \end{bmatrix}\in H$$

ينتج من (١-٢-٤) أن H حلقة جزئية من $M_{2\times2}(\mathbb{Z})$. والآن نعرف

$$\varphi : \mathbb{Z}[\sqrt{2}] \to H$$

$$a+b\sqrt{2} \mapsto \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$$

واضح أن φ راسم غامر (شامل ، فوقى) ، وكذلك راسم واحد لواحد .

$$\forall a+b\sqrt{2}, c+d\sqrt{2}\in \mathbb{Z}[\sqrt{2}]:$$

$$\varphi((a+b\sqrt{2})+(c+d\sqrt{2})) = \varphi(a+c+(b+d)\sqrt{2}) = \begin{bmatrix} a+c & 2(b+d) \\ b+d & a+c \end{bmatrix}$$

$$=\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}+\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}=\varphi(a+b\sqrt{2})+\varphi(c+d\sqrt{2}),$$

$$\varphi((a+b\sqrt{2})(c+d\sqrt{2})) = \varphi(ac+2bd+(ad+bc)\sqrt{2})$$

$$=\begin{bmatrix} ac+2bd & 2(ad+bc) \\ (ad+bc) & ac+2bd \end{bmatrix}$$

$$=\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}=\varphi(a+b\sqrt{2})\varphi(c+d\sqrt{2})$$

أى أن φ هومومورفيزم حلق وبالتالى أيزومورفيزم حلق .

مثال ١٨ : ليكن $\varphi : R \to S$ هومومورفيزم حلق . برهن على أن نواة (φ) $(Ker\ (\varphi))$ مثالى فى R .

البرهان : $Ker(\varphi) := \{a \in R \mid \varphi(a) = 0'\}$

$$= \varphi^{-1}(\{0'\})$$

لكن $\{0'\}$ مثالى فى الحلقة S ، ومن مثال ١١ (ب) يكون $Ker\ (\varphi)$ مثالى فى الحلقة R .

مثال ١٩ : هل يمكن أن تكون نواة هومومورفيزم حلق من $\mathbb{R}$ إلى حلقة K هى $\mathbb{Z}$ ؟

الحل : لايمكن أن يحدث هذا، لأنه من مثال ١٨ السابق مباشرة تكون نواة الهومومورفيزم مثالياً فى $\mathbb{R}$ ، $\mathbb{Z}$ ليست مثالياً فى $\mathbb{R}$ ، فمثلاً $1 \in \mathbb{Z}$ ، $\frac{1}{2} \in \mathbb{R}$ لكن $\frac{1}{2} = 1.\frac{1}{2} \notin \mathbb{Z}$.

مثال ٢٠ : برهن أو انف :

$\varphi : R \to S$ هومومورفيزم حلق ، $A \subset R$ مثالى $\Leftarrow$ $\varphi(A) \subset S$ مثالى .

الحل : التقرير خاطئ مثال مضاد : $\begin{matrix} \iota : \mathbb{Z} \to \mathbb{Q} \\ z \mapsto z \end{matrix}$ راسم التضمين (inclusion mapping)

وهو هومومورفيزم. $\mathbb{Z} \subset \mathbb{Z}$ مثالى ، $\mathbb{Z} \subset \mathbb{Q}$ حلقة جزئية ، لكنها ليست مثالياً فى $\mathbb{Q}$ ، $\iota(\mathbb{Z}) = \mathbb{Z}$

لاحظ أن ι ليس راسما غامراً . انظر مثال١١ (أ) السابق

مثال ٢١ : اضرب مثالاً لحلقة ليس لها عنصر الوحدة وهى محتواه فى حقل .

الحل : الحلقة $2\mathbb{Z}$ داخل $\mathbb{Q}$ أو $\mathbb{R}$ أو $\mathbb{C}$

مثال ٢٢ : هل يمكن أن توجد حلقة إبدالية لها عنصر الوحدة المختلف عن الصفر ، لكنها ليست نطاقاً متكاملاً وتكون محتواة فى حقل ؟

الحل : لايمكن أن توجد مثل هذه الحلقة ، لأنها ستكون ليست خالية من القواسم الصفرية وإلا كانت نطاقاً متكاملاً ، أى أنه يوجد بها a ، b بحيث إن : $a \neq 0 \neq b$ ، $ab = 0$.
لكن a ، b ينتميان إلى حقل، وبالتالى فإنه يوجد a^{-1} (معكوس a الضربى) ، ومن ثم فإن:

$$0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$$

وهذا تناقض

مثال ٢٣ : إذا كانت R حلقة لها عنصر الوحدة 1 ، f هومومورفيزم حلقى من R إلى نطاق متكامل R' ، وإذا كانت نواة (f) لاتساوى R ، فبرهن على أن $f(1)$ سيكون عنصر الوحدة فى R' .

البرهان : نلاحظ أولاً أن $f(1) \neq 0'$ ، وإلا فإنه لجميع $x \in R$ يكون :

$$f(x) = f(1x) = f(1)f(x) = 0'f(x) = 0' \Rightarrow Ker(f) = R \ .$$

وهذا تناقض مع الفرض أن نواة (f) لاتساوى R . كذلك فإن :

$$[f(1)]^2 = f(1)f(1) = f(1.1) = f(1) \qquad (1)$$

والآن ليكن $r' \in R'$ عندئذ فإن :

$$[r'f(1) - r']f(1) = r'[f(1)]^2 - r'f(1) \underset{(1)}{=} 0' \Rightarrow r'f(1) \underset{f(1)\neq 0'}{=} r',$$

R' نطاق متكامل

ومن حيث إن R' حلقة إبدالية فإنه ينتج كذلك أن

$$\forall r' \in R' : f(1)r' = r'$$

ينتج أن $f(1)$ هو عنصر الوحدة R' .

مثال ٢٤ : ليكن A ، B مثاليين فى حلقة R . إذا كان $A \cap B = \{0\}$ ، فبرهن على أن $ab = 0$ عندما يكون $a \in A$ ، $b \in B$

البرهان : $a \in A$ ، $b \in B$ يقتضى أن $ab \in A$ لأن A مثالى ، $b \in B$ يعنى أن $b \in R$. كذلك $ab \in B$ لأن B مثالى ، $a \in A$ يعنى أن $a \in R$ أى أن $ab \in A \cap B = \{0\}$. وينتج المطلوب .

<u>مثال ٢٥</u> : برهن على أن أى حقل لايمكن أن يحتوى مثالياً فعلياً (proper ideal)

<u>البرهان</u> : ليكن F حقلاً ، $I \subset F$ مثالياً . سنبرهن على أن $I = \{0\}$ أو $I = F$.

ليكن $I \neq \{0\}$ ، عندئذ فإنه يوجد $a \in I$ ، $a \neq 0$. ولأن F حقل فإنه يوجد $a^{-1} \in F$ ، والآن $1 = a^{-1}a \in I$. والآن لجميع $b \in F$: $b = 1.b \in I$
I مثالى I مثالى

أى أن $F \subset I$ ، ومن التعريف $I \subset F$ ، ومن ثم فإن $I = F$.

<u>مثال ٢٦</u> : برهن على أن أية حلقة غير صفرية لها عنصر الوحدة ، إبدالية ، لاتحتوى على مثاليات فعلية تكون حقلاً .

<u>البرهان</u> : لتكن K حلقة غير صفرية ، إبدالية ، لها عنصر الوحدة ولا تحتوى على مثاليات فعلية . من حيث إن K غير صفرية فإنه يوجد $0 \neq a \in K$. والآن من مثال ٢ فى (١-٢-٧) ينتج أن

$$aK := \{ax \mid x \in K\}$$

مثالى . ومن حيث أن $a \neq 0$ ، K لاتحتوى على مثاليات فعلية فإن $aK = K$. ومن حيث أن $1 \in K$ فإنه يوجد $b \in K$ بحيث أن $ab = 1$. ومن حيث أن K إبدالية فإن $ab = 1 = ba$ ، أى أنه يوجد معكوس ضربى لـ $a \in K$ ، تكون K حقلاً .

<u>مثال ٢٧</u> : فى التعريف (١-٢-٥) فى الجزء (ب) إذا تحقق فقط

$\forall a \in A \quad \forall b \in R : ba \in A$ يقال أن <u>A مثالى أيسر</u> ، وإذا تحقق فقط

$\forall a \in A \quad \forall b \in R : ab \in A$ يقال إن <u>A مثالى أيمن</u> .

ليكن F حقلاً برهن على أن مجموعة المصفوفات التى على الشكل $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ حيث $a,b \in F$ تكون مثالياً أيمن ، لكنها ليست مثالياً أيسر من حلقة المصفوفات من النوع 2×2 التى عناصرها (مداخلها entries) من F .

<u>البرهان</u> : اعتبر الحلقة S :

$$S := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in F \right\}$$

واعتبر المجموعة

$$I := \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \in F \right\}$$

واضح أن $I \neq \phi$. والآن ليكن $\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} \in I$. ينتج أن :

$$\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & 0 \end{bmatrix} \in I$$

أى أن I زمرة جزئية (بالنسبة للجمع) من S .

والآن ليكن $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in I$ ، $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in S$. ينتج أن :

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} . \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \notin I$$

أى أن I ليس مثالياً أيسر فى S .

والآن ليكن $\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \in I$ ، $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in S$. ينتج أن :

$$\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ax + cy & bx + dy \\ 0 & 0 \end{bmatrix} \in I$$

(لاحظ أن $ax + cy, bx + dy \in F$)

أى أن I مثالى أيمن فى S .

<u>**مثال ٢٨**</u> : لتكن R حلقة إبدالية ، $a \in R$. برهن على أن المجموعة

$$S := \{x \in R \mid ax = 0\}$$

مثالى فى R .

البرهان : إذا كان $a=0$ فإن $S=R$ ، لأن كل عنصر $x\in R$ يحقق $0\ \ x=0$ ، وبالتالى تكون S المثالى التافه R . والآن ليكن $a\neq 0$. لاحظ أن $a\ \ 0=0$ أى أن $0\in S$ ، وتكون S غير خالية .

ليكن $x,y\in S$. ينتج أنه $ax=0$ ، $ay=0$ ومن ثم فإن $a(x-y)=ax-ay=0$ وينتج أن $x-y\in S$ ، وتكون S زمرة جزئية (بالنسبة للجمع) من R (1) .

والآن ليكن $r\in R$ ، $x\in S$. ينتج أن $ax=0$. وبالتالى :

$$\left.\begin{aligned} a(xr)=(ax)r=0r=0, \\ a(rx)=a(xr)=0 \end{aligned}\right\rangle xr\in S, rx\in S \qquad (2)$$

R إبدالية

من (1) ، (2) ينتج المطلوب مباشرة . (قارن مع مثال ١ فى (١-٢-٨))

مثال ٢٩ : برهن على أنه يوجد أيزومورفيزم بين حلقة الأعداد المركبة ، وحلقة جزئية من حلقة المصفوفات من النوع 2×2 ، التى مداخلها (عناصرها) أعداد حقيقية

البرهان : نعتبر مجموعة المصفوفات :

$$M:=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b\in\mathbb{R}\right\}$$

واضح أن $M\neq\phi$. سنبرهن أولا على أن M حلقة جزئية من حلقة المصفوفات من النوع 2×2 ، ومداخلها (عناصرها) من $\mathbb{R}$.

$$\forall\begin{pmatrix} a & b \\ -b & a \end{pmatrix},\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\in M:\begin{pmatrix} a & b \\ -b & a \end{pmatrix}-\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} a-c & b-d \\ -(b-d) & a-c \end{pmatrix}\in M,$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}\in M$$

أى أن M حلقة جزئية من الحلقة $M_{2\times 2}(\mathbb{R})$. نعرف :

$$f:\mathbb{C}\to M$$

$$a+ib\mapsto\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

سنبرهن على أن f تشاكل (أيزومورفيزم) :

$\forall a,b,c,d \in R:$

$$f(a+ib+c+id)=f(a+c+i(b+d))=\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

$$=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}+\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=f(a+ib)+f(c+id),$$

$$f((a+ib)(c+id))=f(ac-bd+i(ad+bc))=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

$$=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=f(a+ib)f(c+id)$$

أى أن f هومومورفيزم حلق (1). واضح أن F راسم غامر (شامل ، فوقى) (2) .

كذلك f راسم واحد لواحد ، لأن :

$$f(a+ib)=f(c+id)\Rightarrow\begin{pmatrix} a & b \\ -b & a \end{pmatrix}=\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\Rightarrow a=c,b=d$$

$$\Rightarrow a+ib=c+id\Rightarrow$$

f أيزومورفيزم $\underset{(1),(2)}{\Rightarrow}$ f راسم واحد لواحد

ملحوظة : لأن $(\mathbb{C},+,.)$ حقل فإن M حقل كذلك .

مثال ٣٠ : لتكن $M:=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$. عرف :

$$f : M\to M$$
$$a+b\sqrt{2}\mapsto a-b\sqrt{2}$$

برهن على أن f أوتومورفيزم حلقى .

البرهان : يترك للقارئ التحقق من أن M حلقة . والآن

$\forall a+b\sqrt{2}, c+d\sqrt{2} \in M :$

$f(a+b\sqrt{2}+c+d\sqrt{2}) = f(a+c+(b+d)\sqrt{2}) = a+c-(b+d)\sqrt{2}$

$= a-b\sqrt{2}+c-d\sqrt{2} = f(a+b\sqrt{2})+f(c+d\sqrt{2}),$

$f((a+b\sqrt{2})(c+d\sqrt{2})) = f(ac+2bd+\sqrt{2}(ad+bc)) = ac+2bd-\sqrt{2}(ad+bc)$

$= (a-b\sqrt{2})(c-d\sqrt{2}) = f(a+b\sqrt{2})f(c+d\sqrt{2}) \Rightarrow$ هومومورفيزم $f\,(1)$

$\forall a+b\sqrt{2} \in M\ \exists a-b\sqrt{2} \in M : f(a\text{-}b)\sqrt{2}) = a+b\sqrt{2} \Rightarrow$ غامر(شامل) $f\,(2)$

أيضا

$f(a+b\sqrt{2}) = f(c+d\sqrt{2}) \Rightarrow a-b\sqrt{2} = c-d\sqrt{2} \Rightarrow a-c = (b-d)\sqrt{2}, a,b,c,d \in \mathbb{Z}$

$\Rightarrow a-c = 0 = b-d \Rightarrow a=c, b=d \Rightarrow a+b\sqrt{2} = c+d\sqrt{2}$

$\Rightarrow$ واحد لواحد $f \underset{(1),(2)}{\Rightarrow}$ أوتومومورفيزم f

<u>مثال ٣١</u> : برهن على أن الهومومورفيزمات الوحيدة من $\mathbb{Q}$ إلى $\mathbb{Q}$ هى راسم الوحدة (The identity mapping) ، الراسم الصفرى (يرسم كل العناصر فى 0)

<u>البرهان</u> : ليكن $f : \mathbb{Q} \to \mathbb{Q}$ هومومورفيزم حلق .

$f(1) = 0 \Rightarrow \forall x \in \mathbb{Q} : f(x) = f(1x) = f(1)f(x) = 0f(x)$

$= 0 \Rightarrow$ الراسم الصفرى f

والآن ليكن $f(1) \neq 0$: من مثال ٢٣ نرى أن $f(1)$ هو عنصر الوحدة فى $\mathbb{Q}$ ، أى أن $f(1) = 1$. والآن ليكن n عدداً صحيحا موجبا :

$$f(n) = f(\underbrace{1+1+\ldots+1}_{\text{من الوحدات } n}) \underset{\text{هومومورفيزم } f}{=} \underbrace{f(1)+f(1)+\ldots+f(1)}_{\text{من الحدود } n} = nf(1) = n \quad (1)$$

إذا كان $n = 0$ ، فإن $f(0) = 0$ ، وإلا f ليس هومومورفيزم حلق .

إذا كان n عدداً صحيحاً سالباً ، ضع $n = -m$ ، حيث m عدد صحيح موجب :

$$f(-m) = -f(m) \underset{(1)}{=} -m$$

أى أن : $f(n)=n$

يتبقى إذا كان n عدداً كسرياً . ليكن $n=\frac{p}{q}$ ، حيث $q\neq 0$ ، $p,q\in\mathbb{Z}$:

$$p=q\frac{p}{q}\Rightarrow f(p)=f(q)f(\frac{p}{q})\Rightarrow f(\frac{p}{q})=\frac{f(p)}{f(q)}=\frac{p}{q}$$

لاحظ أن : $(q\neq 0\Rightarrow f(q)=q\neq 0)$

ومن ثم فإن :

$$\forall x\in\mathbb{Q}: f(x)=x$$

أى أن f هو راسم الوحدة على $\mathbb{Q}$.

مثال ٣٢ : لتكن X مجموعة ، f راسم واحد لواحد ، غامر (شامل ، فوقى) من X على حلقة R . سنعرف العمليتين "+" ، "." على X كالآتى :

$$\forall x,y\in X: x+y=f^{-1}(f(x)+f(y)),$$
$$x.y=f^{-1}(f(x).f(y))$$

برهن على أن $(X,+,.)$ حلقة متشاكلة (أيزومورفية) مع R .

البرهان : لأن $f(x),f(y)\in R$ فإن $f^{-1}(f(x)+f(y)), f^{-1}(f(x).f(y))\in X$.

f واحد لواحد ، غامر (شامل ، فوقى) يقتضى أن $f^{-1}(f(x).f(y))$ ، $f^{-1}(f(x)+f(y))$ يعرفان بطريقة وحيدة (uniquely defined) لكل $x,y\in X$.

لاحظ أن تعريفى "+" ، "." يستلزمان أن :

$$\forall x,y\in X: f(x+y)=f(x)+f(y), f(x.y)=f(x).f(y)$$

والآن :

$$\forall x,y,z\in X: f((x+y)+z)=f(x+y)+f(z)=(f(x)+f(y))+f(z)$$
$$= f(x)+(f(y)+f(z))=f(x)+f(y+z)=f(x+(y+z))$$

R حلقة

$$\Rightarrow (x+y)+z=f^{-1}(f((x+y)+z))=f^{-1}(f(x+(y+z)))=x+(y+z)$$

f تناظر أحادى

وبطريقة مشابهة يمكن البرهنة على أن :

$$\forall x,y,z\in X : x+y=y+x,(x.y).z=x.(y.z),$$
$$x.(y+z)=x.y+x.z,(x+y).z=x.z+y.z$$

$f^{-1}(0)$ هو صفر "الحلقة" X لأن :

$$\forall x\in X : x+f^{-1}(0)=f^{-1}(f(x+f^{-1}(0))=f^{-1}(f(x)+ff^{-1}(0))=f^{-1}(f(x)+0)$$
$$=f^{-1}f(x)=x$$

معكوس x هو $f^{-1}(-f(x))$ لأن :

$$x+f^{-1}(-f(x))=f^{-1}(f(x)+ff^{-1}(-f(x))=f^{-1}(f(x)-f(x))=f^{-1}(0).$$

ومن ثم فإن $(X,+,.)$ حلقة .

ومن حيث إن f بالضرورة هومومورفيزم ، تناظر أحادى فإن $X\cong R$.

مثال ٣٣ : ليكن $\varphi:K\to R$ هومومورفيزم حلقى ، حيث K شبه حقل ، R حلقة . برهن على أن φ إما أن يكون راسماً أحادياً (واحداً لواحد) أو أن يكون هو الراسم الصفرى .

البرهان : من مثال ١٨ نعلم أن نواة (φ) هى مثالى فى K ، ومن مثال ٢٥ نعلم أن الحقول (وكذلك بالطبع أشباه الحقول) لاتحتوى من المثاليات إلا التافهة وبهذا يكون : $Ker(\varphi)=\{0\}$ أو $Ker(\varphi)=K$. إذا كان $Ker(\varphi)=\{0\}$ فمعنى هذا أن φ راسم واحد لواحد (أحادى) . أما إذا كان $Ker(\varphi)=K$ فمعنى هذا أن φ الراسم الصفرى .

مثال ٣٤ : ليكن $\varphi:R\to R'$ إبيمورفيزم حلق (ring epimorphism) ، I مجموعة المثاليات $A\subset R$ بحيث إن $Ker(\varphi)\subset A$ ، I' مجموعة جميع المثاليات فى R' .

برهن على أن الراسمين :

$$F:I\to I' \qquad G:I'\to I$$
$$A\mapsto\varphi(A) \quad ، \quad A'\mapsto\varphi^{-1}(A')$$

تناظران أحاديان ، وكلا منهما معكوس الآخر .

البرهان : المطلوب هو اثبات أن $FoG=1_{I'}$.(1) أى أن FoG هو راسم الوحدة على I'، (2) $GoF=1_I$ ، أى أن GoF هو راسم الوحدة على I .

والآن :

$$FoG : I' \to I'$$
$$A' \mapsto (\varphi o \varphi^{-1})A'$$

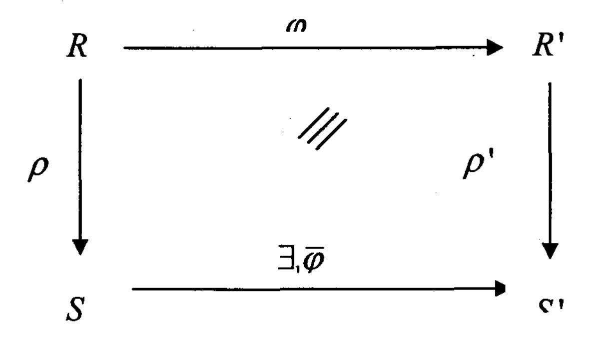
ومن حيث إن φ راسم فوقى (غامر ، شامل) فإن $(\varphi o \varphi^{-1})A' = A'$ أى أن $FoG = 1_{I'}$.

أما

$$GoF : I \to I$$
$$A \mapsto (\varphi^{-1} o \varphi)(A)$$

فنحن نعلم أن $(\varphi^{-1} o \varphi)(A) \supset A$. إذن يتبقى فقط أن نبرهن على أن $(\varphi^{-1} o \varphi)(A) \subset A$. ليكن $x \in (\varphi^{-1} o \varphi)(A) = \varphi^{-1}(\varphi(A))$. هذا يستلزم أن $\varphi(x) \in \varphi(A)$. وهذا يقتضى أنه يوجد $y \in A$ بحيث يكون : $\varphi(x) = \varphi(y) \in \varphi(A)$ وهذا يستلزم أنه يوجد $y \in A$ بحيث يكون : $\varphi(x-y) = \varphi(x) - \varphi(y) = 0$ أى أن $x - y \in Ker(\varphi) \subset A$. ومن حيث إن $y \in A$ ، A مثالى فإن $x \in A$ ، أى أن $(\varphi^{-1} o \varphi)(A) \subset A$. نهاية البرهان .

<u>مثال ٣٥</u> : لتكن R ، R' ، S ، S' حلقات (حلقا) ، وليكن $\rho : R \to S$ ، $\rho' : R' \to S'$ هومومورفيزمين حلقيين . إذا كان ρ غامراً (شاملاً) فإنه لكل هومومورفيزم حلق $\varphi : R \to R'$ بحيث إن $\varphi(Ker(\rho)) \subset Ker(\rho')$ يوجد بالضبط $\overline{\varphi} : S \to S'$ وحيد بحيث يكون الشكل الآتى إبداليا (commutative) :



البرهان : التعريف الآتى لـــ $\overline{\varphi}$ سيجعل الشكل إبداليا :

$$\overline{\varphi}(y) := (\rho' o \varphi)(x), \quad y = \rho(x)$$

$\overline{\varphi}$ معرف جيداً (well defined) : ليكن x_1 ، x_2 بحيث إن $\rho(x_1) = \rho(x_2)$. هذا يقتضى أن $\rho(x_1 - x_2) = \rho(x_1) - \rho(x_2) = 0_S$ ، أى أن : $x_1 - x_2 \in Ker(\rho)$.
ومن حيث إن $\varphi(Ker\rho) \subset Ker(\rho')$ ينتج أن $\varphi(x_1 - x_2) \in Ker(\rho')$ وبالتالى فإن $(\rho' o \varphi)(x_1 - x_2) = 0_{S'}$ أى أن $(\rho' o \varphi)(x_1) = (\rho' o \varphi)(x_2)$.

$\overline{\varphi}$ وحيد (unique) : ليكن $\overline{\varphi}, \psi : S \to S'$ بحيث يتحقق المطلوب .

$$\overline{\varphi} o \rho = \psi o \rho \quad \Rightarrow \quad \overline{\varphi} = \psi$$

ρ غامر (شامل)

$\overline{\varphi}$ هومومورفيزم : لأن ρ راسم غامر (شامل) فإنه لكل $y_1, y_2 \in S$ يوجد $x_1, x_2 \in R$ بحيث إن $y_1 = \rho(x_1), y_2 = \rho(x_2)$. والآن :

$$\overline{\varphi}(y_1 + y_2) = \overline{\varphi}(\rho(x_1) + \rho(x_2)) = \overline{\varphi}(\rho(x_1 + x_2)) = (\overline{\varphi} o \rho)(x_1 + x_2)$$
$$= (\rho' o \varphi)(x_1 + x_2) = \rho'(\varphi(x_1 + x_2)) = \rho'(\varphi(x_1) + \varphi(x_2)) = \rho'(\varphi(x_1)) + \rho'(\varphi(x_2))$$
$$= (\rho' o \varphi)(x_1) + (\rho' o \varphi)(x_2) = (\overline{\varphi} o \rho)(x_1) + (\overline{\varphi} o \rho)(x_2) = \overline{\varphi}(\rho(x_1)) + \overline{\varphi}(\rho(x_2))$$
$$= \overline{\varphi}(y_1) + \overline{\varphi}(y_2)$$

بالمثل لـــ

$$\overline{\varphi}(y_1 . y_2) = \overline{\varphi}(y_1) . \overline{\varphi}(y_2)$$

مثال ٣٦:لتكن R حلقة إبدالية لها على الأقل عنصران ولاتحتوى من المثاليات إلا التافهين. برهن على أن R إما أن تكون حقلاً وإما أنه يوجد عدد أولى p بحيث يكون :

(أ) الزمرة الجمعية فى R (أى $(R, +)$) تكون متشاكلة (أيزومورفية) مع الزمرة $\mathbb{Z}/p\mathbb{Z}$.

(ب) لكل $a, b \in R$: $ab = 0$

البرهان : أولاً ليكن $ab = 0$ لجميع $a, b \in R$. ينتج أن كل زمرة جزئية من $(R, +)$ تكون مثالياً فى R . فينتج من الفرض أن R تحتوى فقط على زمرتين جزئيتين تافهتين (أى لاتحتوى على زمر جزئية فعلية). وبالتالى فإنه ينتج من نظرية لاجرانج (١-١٠-٣) فى نظرية الزمر أن رتبة الزمرة $(R, +)$ عدد أولى p وتكون $(R, +) \cong \mathbb{Z}/p\mathbb{Z}$.

ثانيا : ليكن $a,b \in R$ بحيث إن $a,b \neq 0$. ينتج أن Rb مثالى فى R (انظر مثال٢ فى (١-٢-٧)) بحيث إن $a,b \neq 0$. وهذا يقتضى أن $Rb \neq \{0\}$ ، فينتج من الفرض أن $Rb = R$. وهذا يستلزم أنه يوجد $"1" \in R$ بحيث إن $1b = b$. هذا الـــ "1" هو عنصر الوحدة فى R لأن :

$$Rb = R \Rightarrow \forall x \in R \ \exists y \in R : x = yb, 1x = 1yb = y(1b) = yb = x .$$

ومن حيث إن R تحتوى عنصرين على الأقل فإن $1 \neq 0$.

يتبقى فقط إن نبرهن على أنه لكل $u \in R \setminus \{0\}$ فإنه يوجد $v \in R$ بحيث إن $uv = 1$.

والآن لكل $u \in R \setminus \{0\}$ يكون $Ru \neq \{0\}$ (لأن $u = 1u \in Ru$). Ru مثالى فى R فينتج من الفرض أن

$Ru = R$ ، *أى أنه يوجد* $v \in R$: $vu = 1 = uv$ (لأن $1 \in R$ ، R إبدالية) . نهاية البرهان .

<u>**مثال ٣٧**</u> : برهن على أنه إذا كانت R حلقة ذات عنصر الوحدة 1 ، $\varphi(1) \neq 0'$ (صفر الحلقة R') حيث $\varphi : R \to R'$ هومومورفيزم حلق فإن $\varphi(1) = 1'$ ، حيث $1'$ هو عنصر الوحدة فى $\varphi(R)$.

<u>**البرهان**</u> : لأن R حلقة جزئية (تافهة) من نفسها ، فإن $\varphi(R)$ حلقة جزئية من R' (مثال١١ فى (١-٢-٨)). والآن

$$\varphi(1)\varphi(r) = \varphi(1r) = \varphi(r) = \varphi(r1) = \varphi(r)\varphi(1)$$

(قارن مع مثال ١٠) .

<u>**مثال ٣٨**</u> : ليكن $\varphi : R \to R'$ إبيمورفيزم حلق ، حيث R حلقة لها عنصر الوحدة 1 . ولتكن u وحدة فى R . برهن على أن $\varphi(u)$ وحدة فى R' إذا كانت وفقط إذا كانت u ليست عنصرا فى نواة (φ)

<u>**البرهان**</u> : $\varphi : R \to R'$ هومومورفيزم حلق ، وهو راسم شامل (غامر) فمن مثال ٣٧ السابق مباشرة يكون $\varphi(1) = 1'$ حيث 1 ، $1'$ عنصرا الوحدة فى R ، R' على الترتيب.

والآن $u \in R$ يقتضى أنه يوجد $v \in R$ بحيث يكون $uv = 1$. ومن ثم فإن

$$1' = \varphi(1) = \varphi(uv) = \varphi(u)\varphi(v) \Rightarrow [\varphi(u) \neq 0 \Leftrightarrow \text{وحدة فى } R' \ \varphi(u)]$$

أى أن $\varphi(u)$ وحدة فى R' إذا كانت وفقط إذا كانت $u \notin Ker(\varphi)$.

مثال ٣٩ : برهن على أن كل حلقة لها عنصر وحدة تكون إيزومورفية مع حلقة إندومورفيزمات لزمرة إبدالية .

البرهان : لتكن R حلقة ، لها عنصر الوحدة "1". سنأخذ $(R, +)$ زمرتنا الإبدالية . لكل $a \in R$ نعرف :

$$f_a : R \to R$$
$$x \mapsto ax$$

f_a اندومورفيزم للزمرة " الجمعية " الإبدالية $(R, +)$ لأن :

$$\forall x, y \in R : f_a(x+y) = a(x+y) = ax + ay = f_a(x) + f_a(y)$$

والآن نعرف المجموعة : $E := \{f_a \mid a \in R\}$ وهى حلقة والعمليتان موضحتان فى (1) ، (2) .

سنثبت أولاً أن لجميع $a, b \in R$:

$$f_{a+b} = f_a + f_b \qquad (1)$$
$$f_{ab} = f_a o f_b \qquad (2)$$

لإثبات (1) الذى يعنى أن العملية فى (1) معرفة جيداً :

$$\forall x \in R : f_{a+b}(x) = (a+b)x = ax + bx = f_a(x) + f_b(x) = (f_a + f_b)(x)$$
$$\Rightarrow f_{a+b} = f_a + f_b$$

لإثبات (2) الذى يعنى ان العملية فى (2) معرفة جيداً :

$$f_{ab}(x) = (ab)x = a(bx) = f_a(f_b(x)) = (f_a o f_b)(x) \Rightarrow f_{ab} = f_a o f_b$$

سنثبت الآن أن E حلقة .

$$\forall f_a, f_b, f_c \in E : (f_a + f_b) + f_c \underset{(1)}{=} f_{a+b} + f_c \underset{(1)}{=} f_{(a+b)+c} = f_{a+(b+c)}$$
$$\underset{(1)}{=} f_a + f_{b+c} \underset{(1)}{=} f_a + (f_b + f_c)$$

نعرف العنصر الصفرى $\widehat{0}$ فى E كالآتى $\begin{matrix} \widehat{0} : R \to R \\ x \mapsto 0 \end{matrix}$. واضح أن $\widehat{0}$ إندومورفيزم .

كذلك فإنه لكل $f \in E$ ولكل $x \in R$ يكون

$$(\widehat{0}+f)(x)=\widehat{0}(x)+f(x)=0+f(x)=f(x)\Rightarrow \widehat{0}+f=f$$

نعرف معكوس f_a فى E كالآتى :

$$\forall x\in R:(-f_a)(x):=-f_a(x)$$

والآن :

$$\forall x,y\in R:(-f_a)(x+y):=-f_a(x+y)=-[f_a(x)+f_a(y)]$$
$$=-f_a(y)-f_a(x)=-f_a(x)-f_a(y)=(-f_a)(x)+(-f_a)(y)$$

أى أن $-f_a$ إندومورفيزم . ونثبت أن $(-f_a)$ هو معكوس f_a كالآتى :

$$\forall x\in R:((-f_a)+f_a)(x)=(-f_a)(x)+f_a(x)=-f_a(x)+f_a(x)=0=\widehat{0}(x)$$
$$\Rightarrow (-f_a)+f_a=\widehat{0}$$

ولأى $f_a,f_b\in E$:

$$f_a+f_b=f_{a+b}=f_{b+a}=f_b+f_a$$

ولأى $f_a,f_b,f_c\in E$:

$$(f_a o f_b)o f_c \underset{(2)}{=} f_{ab} o f_c \underset{(2)}{=} f_{(ab)c}=f_{a(bc)} \underset{(2)}{=} f_a o f_{bc} \underset{(2)}{=} f_a o(f_b o f_c),$$

$$f_a o(f_b+f_c) \underset{(1)}{=} f_a o f_{b+c} \underset{(2)}{=} f_{a(b+c)}=f_{ab+ac} \underset{(1)}{=} f_{ab}+f_{ac}=f_a o f_b+f_a o f_c$$

وبالمثل

$$(f_a+f_b)o f_c=f_a o f_c+f_b o f_c$$

أى أن E حلقة .

والآن نعرف الراسم :

$$\varphi:R\to E$$
$$a\mapsto f_a$$

φ هومومورفيزم لأن :

$$\forall a,b\in R:\varphi(a+b)=f_{a+b} \underset{(1)}{=} f_a+f_b=\varphi(a)+\varphi(b),$$
$$\varphi(ab)=f_{ab} \underset{(2)}{=} f_a o f_b=\varphi(a)o\varphi(b)$$

واضح أن φ راسم شامل (غامر ، فوقى) .

كذلك φ راسم أحادى (واحد لواحد) ، لأن :

$$\forall a,b \in R : \varphi(a)=\varphi(b) \Rightarrow f_a = f_b \Rightarrow \forall x \in R : f_a(x) = f_a(y)$$

ولكن R لها عنصر الوحدة "1" ، ومن ثم فإن :

$$f_a(1) = f_b(1) \Rightarrow a = a1 = b1 = b \Rightarrow$$ φ واحد لواحد

وبالتالى فإن φ أيزومومرفيزم . نهاية البرهان .

مثال ٤٠ : وضح كيف تغمر حلقة بلا عنصر وحدة فى حلقة ذات عنصر وحدة (الغمر (embedding) يعنى إدخال الحلقة فى الحلقة ذات عنصر الوحدة بواسطة مونومورفيزم)

الحل : لتكن R حلقة بلا عنصر وحدة . سنكون الآن حلقة ذات عنصر وحدة :

اعتبر $S := \mathbb{Z} \times R$. نعرف العمليتين "+" ، "." كالآتى :

$$\forall (n,r),(m,s) \in S : \quad (n,r)+(m,s) := (n+m, r+s)$$
$$(n,r).(m,s) := (nm, ns+mr+rs),$$

$$ns := \underbrace{s+\ldots+s}_{|n| \text{ من المرات}}$$ ، بالمثل mr

ويترك للقارئ التحقق من أن $(S,+,.)$ حلقة . و $(1, 0)$ هو عنصر الوحدة فيها لأن :

$$\forall (n,r) \in S : \quad (1,0).(n,r) = (1n, 1r + n0 + 0r) = (n,r),$$
$$(n,r).(1,0) = (n1, n0 + 1r + r0) = (n,r)$$

والآن نعرف $\begin{array}{c} f : R \to S \\ r \mapsto (0,r) \end{array}$. f هومومورفيزم لأن :

$$\forall (r,s) \in R : \ f(r+s) = (0, r+s) = (0,r)+(0,s) = f(r)+f(s)$$
$$f(rs) = (0, rs) = (0,r).(0,s) = f(r).f(s)$$

واضح أن f راسم أحادى (واحد لواحد) ،

$R' := \{(0,r) \mid r \in R\} \subset S$ ،

$f(R) = R' \cong R$.

١-٢-٩ : جبر المثاليات

يمكن ببساطة شديدة البرهنة على أن تقاطع عائلة غير خالية من المثاليات (أو المثاليات اليسرى أو المثاليات اليمنى) هو مثالى (أو مثالى أيسر أو مثالى أيمن على الترتيب). وبدهى أن هذا التقاطع هو أكبر مثالى (أو مثالى أيسر أو مثالى أيمن على الترتيب) موجود فى كل هذه المثاليات (أو المثاليات اليسرى أو المثاليات اليمنى على الترتيب) .

وعلى الجانب الآخر فإن تقاطع عائلة غير خالية من المثاليات (أو اليسرى أو اليمنى) التى تحتوى على مجموعة جزئية A من الحلقة هى أصغر مثالى (أو أيسر أو أيمن على الترتيب) يحتوى على المجموعة الجزئية A . ويقال فى هذه الحالة إن هذا المثالى (أو الأيسر أو الأيمن على الترتيب) متولد من A ، ويرمز له بالرمز $[A]$.

نظرية : المثالى الأيسر المتولد من اتحاد المثاليين الأيسرين I_1 ، I_2 فى الحلقة R هو مجموعة العناصر $I_1+I_2 := \{i_1+i_2 \mid i_1\in I_1, i_2\in I_2\}$.

البرهان :

سنبرهن أولاً على أن I_1+I_2 مثالى أيسر . واضح أن $I_1+I_2\neq\phi$. ليكن $a_1+a_2\in I_1+I_2$ ، حيث $a_1\in I_1$ ، $a_2\in I_2$ ، $b_1+b_2\in I_1+I_2$ حيث $b_1\in I_1$ ، $b_2\in I_2$. من حيث إن I_1 ، I_2 مثاليان أيسران ينتج أن $a_1-b_1\in I_1$ ، $a_2-b_2\in I_2$ ، وينتج أن :

$$a_1+a_2-(b_1+b_2)=a_1-b_1+a_2-b_2\in I_1+I_2 .$$

أى أن I_1+I_2 . زمرة جزئية من الزمرة الجمعية $(R\ +)$.

والآن ليكن $a_1+a_2\in I_1+I_2$ ، حيث $a_1\in I_1$ ، $a_2\in I_2$ ، $r\in R$.

(لأن I_1 ، I_2 مثاليان أيسران فى R) $\quad r(a_1+a_2)=ra_1+ra_2\in I_1+I_2$

فينتج أن I_1+I_2 مثالى أيسر فى R .

من حيث إنه لكل $a_1\in I_1$ يمكن أن نكتب $a_1=a_1+0\in I_1+I_2$ يكون $I_1\subset I_1+I_2$.

وكذلك $I_2\subset I_1+I_2$ فيكون $I_1\cup I_2\subset I_1+I_2$ ويكون المثالى الأيسر المتولد من $I_1\cup I_2$ ، والذى نشير إليه بالرمز $[I_1\cup I_2]$ محتوى فى I_1+I_2 ، أى أن (1) $\quad [I_1\cup I_2]\subset I_1+I_2$

لكن أى مثالى أيسر يتولد من $I_1 \cup I_2$ لابد أن يحتوى على جميع العناصر $a_1 + a_2$ حيث $a_1 \in I_1$ ، $a_2 \in I_2$ وبالتالى يحتوى على المثالى الأيسر $I_1 + I_2$، أى أن: (2) $[I_1 \cup I_2] \supset I_1 + I_2$

من (1) ، (2) ينتج أن : $I_1 + I_2 = [I_1 \cup I_2]$

<u>ملحوظة (١)</u> : بوضوح تام يمكن استبدال كلمة "أيمن" بكلمة "أيسر" ، أو بحذف أيسر من كل ما سبق فى النظرية .

<u>ملحوظة (٢)</u> : ليكن $a \in R$ حلقة ، عندئذ فإن المجموعة

$$\{ra + na \mid r \in R, n \in \mathbb{Z}\}$$

تمثل المثالى الأيسر المتولد من العنصر a ، ونشير إليها بالرمز $[a]$. وإذا كانت R تحتوى على عنصر الوحدة 1 فيكون لدينا :

$$a = 1\,a\,,$$

$$ra + na = ra + n1a = (r + n1)a = sa, s \in R$$

ويكون المثالى الأيسر المتولد من العنصر a فى هذه الحالة هو

$$[a] = \{sa \mid s \in R\}$$

<u>ملحوظة (٣)</u> : لتكن A مجموعة جزئية من حلقة R . عندئذ فإن مجموعة جميع العناصر التى على الشكل

$$r_1a_1 + \ldots + r_ia_i + n_1b_1 + \ldots + n_jb_j\ ,$$

حيث

$$a_1, \ldots, a_i, b_1, \ldots, b_j \in A \text{ ، } n_1, \ldots, n_j \in \mathbb{Z} \text{ ، } r_1, \ldots, r_i \in R$$

تكون المثالى الأيسر المتولد من A أى $[A]$.

وإذا كانت R تحتوى على عنصر الوحدة R فإن المثالى $[A]$ يتكون من العناصر التى على الشكل :

$$r_1a_1 + \ldots + r_ia_i$$

كما سبق فى ملحوظة (٢)

ملحوظة (٤) : المثالى الأيمن المتولد من العنصر a فى الحلقة R هو

$$\{ar+na \mid r\in R, n\in \mathbb{Z}\}$$

أما المثالى المتولد من العنصر a فى الحلقة R فهو

$$\{sar+na \mid r,s\in R, n\in \mathbb{Z}\}$$

تعريف : يعرف حاصل ضرب المثاليين A ، B فى الحلقة R بأنه :

$$\begin{aligned} AB &:= [\{ab \mid a\in A, b\in B\}] \\ &= \{\sum_{finite} a_i b_i \mid a_i\in A, b_i\in B\} \end{aligned}$$

ويمكن البرهنة بسهولة على أن AB مثالى فى R .

مثال ١ : يقال لمثاليين A ، B فى حلقة R إنهما **متعاظمان معاً** (comaximal) إذا كان $A+B=R$.

برهن على أنه إذا كان A ، B مثاليين متعاظمين معاً فى حلقة إبدالية R ذات عنصر الوحدة 1 فإن

$$AB = A\cap B .$$

البرهان :

$$"\subset": x\in AB \Rightarrow x=\sum_{i=1}^{n} a_i b_i, a_i\in A, b_i\in B$$

$$\Rightarrow x=\sum_{i=1}^{n} a_i b_i, a_i b_i\in A, a_i b_i\in B$$ (لأن A ، B مثاليان)

$$\Rightarrow x=\sum_{i=1}^{n} a_i b_i, a_i b_i\in A\cap B \Rightarrow x\in A\cap B \Rightarrow AB\subset A\cap B \qquad (1)$$

$$"\supset": A+B=R\ni 1 \Rightarrow \exists a\in A\ \exists b\in B: a+b=1$$ (عنصر الوحدة فى R)

$$x\in A\cap B \Rightarrow x\in A, x\in B .$$

$$x = 1x = (a+b)x = a^{\in A} x^{\in B} + b^{\in B} x^{\in A} \in AB$$ (لأن R حلقة إبدالية)

$$\Rightarrow A\cap B\subset AB \qquad (2)$$

(1) ، (2) تعطيان النتيجة مباشرة .

١-٢-١٠ تعريف :

يقال لمثالى A فى حلقة R إنه **مثالى أساسى** (principal ideal) إذا وجد $a \in R$ بحيث يكون $A=[a]$ (انظر (١-٢-٩)) . ويقال إنه **منتهى التولد** (finitely generated) إذا وجد $a_1, a_2, ..., a_n \in R$ بحيث يكون : $A=[a_1, a_2, ..., a_n]$.

ويقال لحلقة R إنها **نطاق مثاليات أساسية** (principal ideal domain) إذا كانت R نطاقاً متكاملاً ، وكان كل مثالى فيها مثالياً أساسياً .

ويقال لحلقة إنها **حلقة نويترية** (Noetherian ring) إذا كان كل مثالى فيها منتهى التولد .

ويقال لحلقة إنها **حلقة أرتينينية** (Artinian ring) إذا كانت كل سلسلة متنازلة $A_0 \supset A_1 \supset A_2 \supset ...$ من المثاليات فى R متوقفة ، أى أنه يوجد $n \in \mathbb{N}$ بحيث يكون $A_{k+n} = A_n \quad \forall k \in \mathbb{N}$

١-٢-١١ نظرية : لتكن R حلقة . التقريرات الآتية متكافئة :

(١) R نويترية

(٢) كل سلسلة متصاعدة $A_0 \subset A_1 \subset A_2 \subset ...$ من المثاليات فى R تكون متوقفة ، أى أنه يوجد $n \in \mathbb{N}$ بحيث يكون : $A_{n+k} = A_n \quad \forall k \in \mathbb{N}$

(٣) كل مجموعة غير خالية I من المثاليات فى R تحتوى على عنصر أعظم ، أى أنه يوجد $B \in I$ بحيث إنه لايوجد $A \in I$: $B \subsetneq A \subsetneq R$

البرهان : "(١) $\Leftarrow$ (٢)" : لأى سلسلة متصاعدة $A_0 \subset A_1 \subset A_2 \subset ...$ من المثاليات فى R المجموعة $A = \bigcup_{k \in \mathbb{N}} A_k$ تكون مثالياً فى R (لاحظ أنه إذا كان A_1 ، A_2 مثاليين فى حلقة R فإن : $A_2 \subset A_1$ أو $A_1 \subset A_2 \Leftrightarrow$ مثالى $A_1 \cup A_2 \subset R$) . والآن لأن R نويترية فإنه يوجد $a_1, a_2, ..., a_\ell \in R$ بحيث إن : $A=[a_1, a_2, ..., a_\ell]$. ومن تعريف A فإنه لكل $i \in \{1,2,...,\ell\}$ يوجد $n_i \in \mathbb{N}$ بحيث إن $a_i \in A_{n_i}$. وإذا كان n هو أكبر

هذه الأعداد الطبيعية n_1 ، n_2 ، ... ، n_ℓ فإنه لكل $i \in \{1,2,...,\ell\}$: $a_i \in A_n$. وبالتالى فإن $A=[a_1,a_2,...,a_\ell] \subset A_n$ ولكن $A_{n+k} \subset A$ فيكون لدينا : $A_{n+k} \subset A \subset A_n$ لكل $k \in \mathbb{N}$. ومن ثم فإن $A_{n+k} = A_n$ لكل $k \in \mathbb{N}$.

"(٢) $\Leftarrow$ (٣)": إذا لم يوجد عنصر أعظم فى مجموعة غير خالية من المثاليات فى R ، فإننا نستطيع أن ننشئ سلسلة متصاعدة من المثاليات $A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq ...$ من عناصر I ، وهى غير متوقفة

"(٣) $\Leftarrow$ (١)": ليكن $A \subset R$ مثاليا ، ولتكن I هى مجموعة جميع المثاليات منتهية التولد والتى تكون محتواة فى A . لاحظ أن $\{0\} \in I$ ، أى أن I غير خالية .

(٣) تستلزم وجود عنصر أعظم ، وليكن هو τ . ولأن $\tau \in I$ فإنه يوجد $c_1, c_2,...,c_n \in R$ بحيث إن: $\tau = [c_1, c_2,...,c_n]$. سيكون المثالى A منتهى التولد إذا برهنا على أن $A = \tau$. لاحظ أولاً أن $\tau \subset A$ لأن $\tau \in I$. وثانياً فليكن $a \in A$ عنصراً اختيارياً . المثالى $\tau' := [c_1,...,c_n, a]$ منتهى التولد ويكون أيضاً محتوى فى A ، أى أنه عنصر فى I . ولكن τ هو عنصر أعظم فى I ، $\tau \subset \tau'$ وبالتالى فإن $\tau = \tau'$ ، ومن ثم فإن $a \in \tau$ أى أن $A = \tau$.

<u>**١-٢-١٢ نتيجة**</u> : ليكن $\varphi : R \to R'$ إيبيمورفيزم حلق .

R حلقة نويترية $\Leftarrow$ R' حلقة نوترية .

<u>**البرهان**</u> : لتكن $A_1' \subset A_2' \subset A_3' \subset ...$ سلسلة متصاعدة من المثاليات فى R' . لكل $i \in \mathbb{N}$ نعرف $A_i := \varphi^{-1}(A_i')$ (مثالى من مثال ١١ فى (١-٢-٨)) مثالى فى R ، ويكون $A_1 \subset A_2 \subset A_3 \subset ...$. والآن R حلقة نويترية يستلزم أن السلسلة $A_1 \subset A_2 \subset A_3 \subset ...$ تكون متوقفة . ولكن φ إيبيمومورفيزم يستلزم أن $A_1' \subset A_2' \subset A_3' \subset ...$ تكون سلسلة من المثاليات حيث $(\varphi o \varphi^{-1})(A_i') = \varphi(\varphi^{-1}(A_i')) = \varphi(A_i) = A_i'$ لكل $i \in \mathbb{N}$ التى تكون متوقفة كذلك .

١-٢-١٣ أمثلة :

(١) $\mathbb{Z}$ نطاق مثاليات أساسية. $\mathbb{Z}$ نطاق متكامل ، كل مثالى فى $\mathbb{Z}$ هو مثالى أساسى فيها:

$$A \subset \mathbb{Z} \text{ مثالى } \Leftrightarrow \exists m \in \mathbb{N} : A = m\mathbb{Z}$$

وبالتالى فإن $\mathbb{Z}$ تكون حلقة نويترية .

(٢) أى شبه حقل يكون حلقة نويترية وأرتينية ، لأنه لايوجد فى شبه الحقل مثاليات إلا المثاليان التافهان : شبه الحقل نفسه ، $\{0\}$

(٣) $\mathbb{Z}$ ليست حلقة أرتينية : السلسلة

$$\mathbb{Z} \underset{\neq}{\supset} 2\mathbb{Z} \underset{\neq}{\supset} 2^2\mathbb{Z} \underset{\neq}{\supset} 2^3\mathbb{Z} \underset{\neq}{\supset} \ldots$$

ليست متوقفة

١-٢-١٤ ملحوظة :

رأينا فى الأمثلة السابقة مباشرة حلقة نويترية لكنها ليست أرتينية . فى الحلقات (ذات عنصر الوحدة !) العكس ليس موجوداً ، أى أنه لايوجد فيها حلقة أرتينية لكنها ليست نويترية .

١-٢-١٥ أمثلة محلولة :

مثال ١ : اضرب مثالاً لبيان أن الحلقات الجزئية من الحلقات النويترية ليست بالضرورة نويترية

الحل : المجموعة $M(\mathbb{C})$: مجموعة كل الدوال الميرومورفية(meromorphic) على $\mathbb{C}$ تكون حقلاً ، وبالتالى فهى حلقة نويترية .

لكن المجموعة $H(\mathbb{C})$ مجموعة الدوال الهولومورفية (holomorphic) (التحليلية (analytic) ، القابلة للتفاضل (differentiable)) ليست نويترية . ولبيان ذلك : لكل $n \in \mathbb{N}$ نعرف :

$$A_n := \{f \in H(\mathbb{C}) \mid f(n+k) = 0 \quad \forall k \in \mathbb{N}\}$$

$A_n \subset H(\mathbb{C})$ مثالى لأن: الدالة الصفرية $\widehat{0}$ تحقق بالطبع $\widehat{0}(n+k)=0$ لجميع $k \in \mathbb{N}$ وهى دالة هولومورفية .

كذلك فإنه لجميع f ، h دالتين هولومورفيتين ، $f,h \in A_n$:

$$(f-h)(n+k)=f(n+k)-h(n+k)=0 \quad \forall k \in \mathbb{N} \Rightarrow f-h \in A_n$$

ولجميع $f \in A_n$ ، $g \in H(\mathbb{C})$ يتحقق :

$$(gf)(n+k)=g(n+k)f(n+k)=g(n+k)0=0 \Rightarrow gf \in A_n$$

وبالمثل $fg \in A_n$ والآن لدينا

$$A_0 \subset A_1 \subset A_2 \subset \ldots$$

وينتج من نظرية فايرشتراس لحاصل الضرب (Weierstrass product theorem) أنه لكل $n \in \mathbb{N}$ يوجد $f \in H(\mathbb{C})$ بحيث إن $f(n)=1$ ، $f(n+k)=0 \quad \forall k \in \mathbb{N}\setminus\{0\}$

وهكذا نحصل على

$$A_0 \underset{\neq}{\subset} A_1 \underset{\neq}{\subset} A_2 \underset{\neq}{\subset} \ldots$$

وهى غير متوقفة .

<u>مثال ٢</u> : برهن على أن الحلقة $C(\mathbb{R})$ (حلقة كل الدوال المتصلة من $\mathbb{R}$ إلى $\mathbb{R}$ ليست نويثرية .

<u>البرهان</u> : لكل $n \in \mathbb{N}\setminus\{0\}$ نعرف

$$A_n := \{f \in C(\mathbb{R}) : f \,|\, [0,\frac{1}{n}] = 0\}$$

A_n مثالى فى $C(\mathbb{R})$ لأن الدالة الصفرية $\widehat{0}$ تحقق الشرط $\widehat{0} \,|\, [0,\frac{1}{n}]=0$ ، وهى دالة متصلة بالطبع كذلك فإنه لجميع $f,g \in A_n$ يكون $f-g \in A_n$. كذلك فإنه لجميع $f \in A_n$ ، $g \in C(\mathbb{R})$ يكون $fg, gf \in A_n$ $\begin{pmatrix} (fg)(x) := f(x)g(x). \\ g(x)f(x) := (gf)(x) \quad \forall x \in \mathbb{R} \end{pmatrix}$

والآن من الواضح أن السلسلة

$$A_1 \underset{\neq}{\subseteq} A_2 \underset{\neq}{\subseteq} A_3 \underset{\neq}{\subseteq} \ldots$$

غير متوقفة (واضح أن $A_n \underset{\neq}{\subseteq} A_{n+1} \forall n \in \mathbb{N}$)

مثال ٣ : فى النظرية (١-٢-١١) برهن على أن التقرير (٢) يستلزم التقرير (١) مباشرة أى دون المرور على (٣)

البرهان : ليكن التقرير (٢) متحققاً . وليكن هناك مثالياً I ليس منتهى التولد. وليكن $a_1 \in I$. نظراً لأن I غير منتهى التولد ، فإن $[a_1]$ مجموعة جزئية فعلية من I ، فنستطيع أن نختار $a_2 \in I$ بحيث يكون $a_2 \notin [a_1]$. وكما سبق فإن $[a_1, a_2]$ يكون مجموعة جزئية فعلية من I ، ونختار $a_3 \in I$ بحيث يكون $a_3 \notin [a_1, a_2]$. وبالاستمرار نستطيع أن نكون السلسلة غير المتوقفة

$$[a_1] \underset{\neq}{\subseteq} [a_1, a_2] \underset{\neq}{\subseteq} [a_1, a_2, a_3] \ldots$$

تمارين

(١) برهن على أن تقاطع حلقات جزئية فى حلقة R يكون حلقة جزئية فى R

(٢) برهن أو انف : اتحاد حلقتين جزئيتين من حلقة R يكون حلقة جزئية فى R

(٣) برهن على أن تقاطع مثاليات فى حلقة R يكون مثالياً فى R

(٤) برهن أو انف : اتحاد مثاليين فى حلقة R يكون مثالياً فى R

(٥) اوجد جميع الهومومورفيزمات $\varphi : \mathbb{Z} \to \mathbb{Z}$

(إرشاد : يتعين الهومومورفيزم من صورة المولد فى الزمرة $(\mathbb{Z}, +)$ ، أى يتعين من $\varphi(1)$. ضع $\varphi(1) = n$. واضح أن $\varphi(1) = 0$ ، $\varphi(1) = 1$ يعطيان هومومورفيزمين هل توجد n أخرى ؟)

(٦) ليكن $m, n \in \mathbb{N}$ ، ليكن k هو المضاعف المشترك الأصغر لـــ m ، n . برهن على أن $m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$ (تذكر أن $n\mathbb{Z}$ حلقة جزئية من $\mathbb{Z}$)

(٧) لتكن $M_{2\times2}(\mathbb{Z})$ حلقة جميع المصفوفات من النوع 2×2 على الأعداد الصحيحة ، ولتكن

$$R := \left\{ \begin{pmatrix} a & a+b \\ a+b & b \end{pmatrix} \mid a,b \in \mathbb{Z} \right\}$$

برهن أو انف : R حلقة جزئية من $M_{2\times2}(\mathbb{Z})$

(٨) لتكن $M_{2\times2}(\mathbb{Z})$ مثلما هى فى تمرين (٧) السابق مباشرة . ولتكن

$$R := \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} \mid a,b \in \mathbb{Z} \right\}$$

برهن أو انف : R حلقة جزئية من $M_{2\times2}(\mathbb{Z})$

(٩) لتكن R حلقة ذات عنصر الوحدة e . برهن على أن

$$S = \{ne \mid n \in \mathbb{Z}\}$$

حلقة جزئية من R

(١٠) هل الراسم

$$\varphi : \mathbb{Z} \to 2\mathbb{Z}$$
$$x \mapsto 2x$$

هومومورفيزم زمر من $(\mathbb{Z},+)$ إلى $(2\mathbb{Z},+)$ ؟ هل هو هومومورفيزم حلق من $(\mathbb{Z},+,.)$ إلى $(2\mathbb{Z},+,.)$ ؟

(١١) فى الحلقة $\mathbb{Z}$ اوجد عدداً صحيحاً موجباً a بحيث يكون :

(أ) $[a] = [2] + [3]$

(ب) $[a] = [3] + [6]$

(جـ) $[a] = [m] + [n]$

(١٢) ليكن A ، B مثاليين فى حلقة R . برهن على أن حاصل الضرب AB المعرف كالآتى:

$$AB := \{a_1b_1 + a_2b_2 + \ldots + a_nb_n \mid a_i \in A, b_i \in B, \quad n \text{ عدد صحيح موجب}\}$$

يكون مثاليا فى R

(١٣) اوجد عدداً صحيحاً موجباً a بحيث يكون

(أ) $[a]=[3]\,[4]$

(ب) $[a]=[6]\,[8]$

(جـ) $[a]=[m]\,[n]$

(١٤) لتكن R حلقة لها عنصر الوحدة 1 . وليكن A مثالياً فى R يحتوى على "1" . برهن على أن $A=R$

(١٥) برهن على أن العناصر منعدمة القوة (انظر مثال ١٢ فى (١-١-١٥)) فى حلقة إبدالية R تكون حلقة جزئية من R

(١٦) ليكن R نطاقاً متكاملاً ، $a,b\in R$ ، $b\neq 0$ ، a ليس وحدة . برهن على أن $[ab]\subsetneq[b]$.

(١٧) هل $\mathbb{Z}_6$ حلقة جزئية من $\mathbb{Z}_{12}$ ؟

(١٨) لتكن R حلقة ، p عدداً أولياً ثابتاً . برهن على أن

$$I_p := \left\{ r\in R \;\middle|\; \begin{array}{l}\text{الرتبة الجمعية لـــ } r \text{ هى قوة من قوى } p\\ \text{(أى هى } p^n \text{ لبعض } n \text{ عدد صحيح موجب)}\end{array} \right\}$$

برهن على أن I_p مثالى فى R

(١٩) لتكن R حلقة إبدالية ، $a,b\in R$. برهن على أن :

$$\{x\in R \mid ax\in bR\}$$

مثالى فى R

لتكن $M_{2\times2}(\mathbb{R})$ حلقة جميع المصفوفات من النوع 2×2 وعناصرها أعداد حقيقية .

(٢٠) ليكن $\varphi:\mathbb{C}\to M_{2\times2}(\mathbb{R})$ معرفاً كالآتى :

$$\varphi(a+ib)=\begin{pmatrix} a & b\\ -b & a\end{pmatrix}$$

حيث $a,b\in\mathbb{R}$. برهن على أن φ أيزومورفيزم

(٢١) برهن على أن الراسم $\begin{aligned}\varphi:\mathbb{C}&\to\mathbb{C}\\ a+ib&\mapsto a-ib\end{aligned}$ أيزومورفيزم

(٢٢) برهن على أن $2\mathbb{Z}$ تتشاكل مع $\mathbb{Z}$ كزمرتين ، ولكنهما لاتتشاكلان كحلقتين .

(٢٣) برهن على أن الراسم $\begin{aligned}\varphi:\mathbb{R}[X]&\to\mathbb{R}\\ P[X]&\mapsto P(1)\end{aligned}$ ($\mathbb{R}[X]$ هى حلقة كثيرات الحدود ذات المعاملات الحقيقية) إبيمورفيزم . ما نواته ؟

(٢٤) برهن على أنه إذا كان m,n عددين صحيحين موجبين مختلفين ، فإن الحلقتين $m\mathbb{Z}$ ، $n\mathbb{Z}$ لايمكن أن تكونا متشاكلتين .

(٢٥) ليكن $f:R\to S$ هومومورفيزم حلق . برهن على أن :

(أ) f مونومورفيزم $\Leftrightarrow$ [$\forall T$ حلقة $\forall g,h:T\to R$ هومومورفيزمين $fg=fh\Rightarrow g=h$]

(ب) f إبيمورفيزم $\Leftrightarrow$ [$\forall T$ حلقة $\forall g,h:S\to T$ هومومورفيزمين $gf=hf\Rightarrow g=h$]

٣-١ الحلقات العاملة Factor rings

من حيث إن الزمرة الجمعية $(R,+)$ فى الحلقة R إبدالية ، فإن كل مثالى فى الحلقة R يكون زمرة جزئية طبيعية . وبالتالى فإننا نستطيع أن نكون الزمرة العاملة

$$R/A := \{x + A \mid x \in R\}, \quad A \text{ مثالى}$$

حيث

$$\forall x, y \in R : (x + A) + (y + A) = x + y + A$$

(انظر الزمر العاملة (١-٧) فى نظرية الزمر)

<u>١-٣-١ نظرية</u> :

لتكن R حلقة ، A مثالى فى R ، $\begin{aligned}\rho : R &\to R/A \\ x &\mapsto x + A\end{aligned}$ إبيمورفيزم الزمر الطبيعى (canonical group epimorphism) . عندئذ فإنه توجد بالضبط عملية وحيدة "." على R/A بحيث تكون $(R/A,+,.)$ حلقة ، ويكون ρ إبيمورفيزم حلق .

البرهان : إذا كانت $(R/A,+,.)$ حلقة ، ρ هومومورفيزم حلق ، فإنه لجميع $x,y \in R$ يتحقق:

$$(x + A).(y + A) = \rho(x).\rho(y) \quad = \quad \rho(xy) = xy + A$$

ρ هومومورفيزم

أى أنه <u>توجد على الأكثر عملية واحدة فى</u> R/A تحقق الخصائص المنشودة .

وسنثبت الآن أنه توجد بالفعل هذه العملية .

ولإثبات <u>وجود</u> هذه العملية فى R/A :

$$\forall x, y \in R : (x + A).(y + A) = xy + A$$

يجب أن نبرهن على أن هذه العملية "معرفة جيداً" (well-defined) كالآتى :

ليكن $x'+A=x+A$ ، $y'+A=y+A$. المطلوب هو البرهنة على أن $x'y'+A=xy+A$ (يقال إن العملية لاتعتمد على الممثلين)

(The operation does not depend on the representatives)

والآن :

$$x'+A=x+A, y'+A=y+A \Rightarrow \exists r,s\in A : x'=x+r, y'=y+s$$ (لأن $0\in A$)

$$\Rightarrow x'y'+A=(x+r)(y+s)+A=xy+xs+ry+rs+A = xy+A$$

(A مثالى)

أى أن العملية معرفة جيداً . ونثبت قانون المشاركة (التجميع) فى عملية الضرب كالآتى :

$$\forall\, x,y,z\in R : ((x+A).(y+A)).(z+A)=(xy+A).(z+A)=(xy)z+A$$

$$= x(yz)+A=(x+A).(yz+A)=(x+A).((y+A).(z+A))$$

R حلقة

ولإثبات قانونى التوزيع :

$$\forall x,y,z\in R : (x+A).[(y+A)+(z+A)]=(x+A).(y+z+A)$$

$$=x(y+z)+A = xy+xz+A=xy+A+xz+A=$$

R حلقة

$$=(x+A).(y+A)+(x+A).(z+A)$$

وبالمثل يثبت أن :

$$[(x+A)+(y+A)].(z+A)=(x+A).(z+A)+(y+A).(z+A)$$

والآن إذا كانت R إبدالية فإن R/A تكون إبدالية لأن :

$$\forall x,y\in R : (x+A).(y+A)=xy+A = yx+A=(y+A).(x+A)$$

R إبدالية

وإذا كانت R لها عنصر الوحدة "1" ، فإن R/A لها عنصر الوحدة $1+A$ لأن :

$$\forall x\in R : (1+A).(x+A)=1x+A=x+A,$$

$$(x+A).(1+A)=x1+A=x+A$$

نهاية البرهان .

تسمى الحلقة $(R/A,+,.)$ الحلقة العاملة من R بالنسبة إلى A

(The factor ring of R w.r.t. A) أو حلقة فصول البواقى لـــ R مقياس A

(The residue class ring of R modulo A)

<u>**١-٣-٢ ملحوظة**</u> : $R \supset A$ مثالى $\Leftrightarrow [\exists R'$ حلقة $\exists \varphi : R \to R'$ هومومورفيزم حلق

بحيث يكون $Ker(\varphi) = A]$

البرهان : "$\Rightarrow$" : ليكن $A \subset R$ مثاليا . نعرف الحلقة $R' := R/A$ ، $\varphi : R \to R/A$
$x \mapsto x + A$

"$\Leftarrow$" : نعلم أن نواة (φ) $(Ker(\varphi))$ زمرة جزئية طبيعية فى $(R,+)$ (انظر (١-٦-٤) فى نظرية الزمر) . وسنبرهن الآن على أنها مثالى فى R :

$$\forall r \in R \ \ \forall x \in Ker(\varphi) : \varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0 \Rightarrow rx \in Ker(\varphi).$$

وبالمثل $xr \in Ker(\varphi)$. (انظر مثالى ١١ ، ١٨ فى (١-٢-٨))

<u>**١-٣-٣ نظرية الهومومورفيزم**</u> : <u>**The homomorphism theorem**</u>

$$\varphi : R \to R' \text{ هومومورفيزم حلق } \Rightarrow \varphi(R) \cong R/Ker(\varphi)$$

<u>**البرهان**</u> :

اعتبر
$$\psi : R/Ker(\varphi) \to \varphi(R)$$
$$x + Ker(\varphi) \mapsto \varphi(x)$$

نلاحظ أن $Ker(\varphi)$ مثالى فى R وبالتالى وحسب ماسبق تكون $R/Ker(\varphi)$ حلقة كما أن $R \subset R$ حلقة جزئية ، وتكون $\varphi(R)$ حسب مثال ١١ فى (١-٢-٨) أيضاً حلقة .

والآن نبرهن على أن ψ أيزومورفيزم حلق كالآتى :

ψ <u>**معرف جيداً**</u> : $\forall x, y \in R : x + Ker(\varphi) = y + Ker(\varphi)$

(لأن $0 \in Ker(\varphi)$) $\Rightarrow x - y \in Ker(\varphi)$

$$\Rightarrow 0 = \varphi(x - y) = \varphi(x) - \varphi(y) \Rightarrow \varphi(x) = \varphi(y)$$

أى أن "الصور" (images) لاتعتمد على "الممثلين" (representatives)

ψ **هومومورفيزم حلق** :

$$\forall x, y \in R: \quad \psi((x + Ker(\varphi)) + (y + Ker(\varphi)) \quad = \quad \psi(x + y + Ker(\varphi))$$

(١-٧-١) نظرية الزمر

$$= \varphi(x + y) = \varphi(x) + \varphi(y) = \psi(x + Ker(\varphi)) + \psi(y + Ker(\varphi)).$$

$$\psi((x + Ker(\varphi)).(y + Ker(\varphi))) \quad = \quad \psi(xy + Ker(\varphi)) = \varphi(xy) = \varphi(x)\varphi(y)$$

١-٣-١

$$= \psi(x + Ker(\varphi))\psi(y + Ker(\varphi))$$

ψ **غامر (شامل ، فوقى)** : واضح !

ψ **واحد لواحد (أحادى)** :

$$\forall x, y \in R: \psi(x + Ker(\varphi)) = \psi(y + Ker(\varphi)) \Rightarrow \varphi(x) = \varphi(y) \Rightarrow$$

$$\varphi(x - y) = \varphi(x) - \varphi(y) = 0' \Rightarrow x - y \in Ker(\varphi) \Rightarrow x + Ker(\varphi) = y + Ker(\varphi).$$

($0'$ العنصر الصفرى فى $\varphi(R)$)

١-٣-٤ النظرية الأولى للأيزومورفيزم **The first isomorphism theorem**

ليكن $A \subset R$ مثالياً فى الحلقة R ، $B \subset R$ حلقة جزئية داخلها . ينتج أن :

$$(A + B)/A \cong B/A \cap B$$

البرهان : نبرهن أولاً على أن $A + B \subset R$ حلقة جزئية كالآتى :

$$\phi \neq A + B := \{a + b \mid a \in A, b \in B\} \qquad (0 = 0 + 0 \in A + B)$$

والآن لجميع $a_1, a_2 \in A$ ، $b_1, b_2 \in B$:

$$a_1 + b_1 - (a_2 + b_2) = a_1 - a_2 + b_1 - b_2 \in A + B \quad (A \text{ مثالى ، } B \text{ حلقة جزئية فى } R)$$

$$(a_1 + b_1)(a_2 + b_2) = a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2 \in A + B$$

(لأن $b_1b_2 \in B$ ، $a_1a_1, a_1b_2, b_1a_2 \in A$)

كذلك لأن A مثالى فى R ، $A \subset A+B \subset R$ ، $A+B$ حلقة جزئية من R فإن A يكون مثالياً فى $A+B$

وبالتالى فإن التكوين $(A+B)/A$ يعرف حلقة (١-٣-١)

والآن نعرف

$$\varphi : B \to (A+B)/A$$
$$b \mapsto b+A$$

φ <u>معرف جيداً</u> : واضح

φ <u>غامر (شامل)</u> : واضح أيضاً ، لأن أى عنصر فى $A+B/A$ سيكون على الشكل $a+b+A$ حيث $a \in A$ ، $b \in B$ ، وَهذا العنصر يكون هو نفسه $b+A$. ومن ثم فإنه يوجد $b \in A$ بحيث إن $\varphi(b)=b+A$

φ <u>هومومورفيزم حلق</u> :

$$\forall b_1, b_2 \in B: \quad \varphi(b_1+b_2)=b_1+b_2+A=b_1+A+b_2+A$$
$$=\varphi(b_1)+\varphi(b_2).$$
$$\varphi(b_1b_2)=b_1b_2+A \underset{1-3-1}{=} (b_1+A).(b_2+A)=\varphi(b_1).\varphi(b_2)$$

والآن نحسب نواة (φ) :

$$Ker(\varphi)=\{b \in B \mid \varphi(b)=b+A=A\}$$

(A هو العنصر الصفرى فى $A+B/A$ حسب (١-٣-١) أو (١-٧) فى نظرية الزمر)

$$=\{b \in B \mid b \in A\}=A \cap B$$

والآن بتطبيق نظرية الهومومورفيزم (١-٣-٣) نحصل على

$$B/A\cap B = B/Ker(\varphi) \cong \varphi(B) \underset{\text{غامر } \varphi}{=} (A+B)/A$$

نهاية البرهان .

١-٣-٥ النظرية الثانية للأيزومورفيزم The second isomorphism theorem

ليكن $A,B \subset R$ مثاليين فى الحلقة R ، $A \subset B$. عندئذ فإن :

$$\frac{R/A}{B/A} \cong R/B$$

البرهان : نلاحظ أن التكوينين R/A ، R/B ممكنان ويعطيان حلقتين . أما التكوين $\frac{R/A}{B/A}$

فلكى يكون ممكناً يجب أن يكون B/A مثالياً فى R/A ، وسنثبت هذا كجزء فى البرهان .

نعرف الراسم :

$$\varphi : R/A \to R/B$$
$$x + A \mapsto x + B$$

φ **معرف جيداً** :

$$\forall x,y \in R : x + A = y + A \Rightarrow x - y \in A \subset B \Rightarrow x + B = y + B$$

أى أن

$$x + A = y + A \Rightarrow \varphi(x + A) = \varphi(y + A)$$

φ **هومومورفيزم حلق** :

$$\forall x,y \in R : \varphi((x + A) + (y + A)) = \varphi(x + y + A) = x + y + B$$

$$= x + B + y + B = \varphi(x + A) + \varphi(x + A)$$

$$\varphi((x+A).(y+A)) = \varphi(xy+A) = xy+B = (x+B)(y+B) = \varphi(x+A)\varphi(y+A)$$

φ **شامل (غامر ، فوقى)** : واضح

والآن نحسب نواة (φ) :

$$Ker(\varphi) = \{x + A \mid \varphi(x + A) = x + B = B\}$$
$$= \{x + A \mid x \in B\} = B/A$$

ومن ثم فإن B/A مثالى فى R/A .

وبتطبيق نظرية الهومومورفيزم (١-٣-٣) نحصل على :

$$\frac{R/A}{B/A} = \frac{R/A}{Ker(\varphi)} = \varphi(R/A) \quad = \quad R/B$$

φ غامر

نهاية البرهان .

١-٣-٦ أمثلة محلولة :

مثال١ : اكتب عناصر $2\mathbb{Z}/6\mathbb{Z}$

الحل :

$$2\mathbb{Z}/6\mathbb{Z} := \{0+6\mathbb{Z}, 2+6\mathbb{Z}, 4+6\mathbb{Z}\}$$

لاحظ أن $6+6\mathbb{Z} = 6\mathbb{Z}$ ، $8+6\mathbb{Z} = 2+6\mathbb{Z}$ ، وهكذا ...

كما أن $6\mathbb{Z}$ مثالى فى $2\mathbb{Z}$.

كما أن $2\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$. ولاحظ أن $\mathbb{Z}/n\mathbb{Z}$ تتشاكل مع $\mathbb{Z}_n$ التى وردت فى مثال ١٠ فى (١-١-١٤).

مثال٢ : لتكن $R := \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i \in \mathbb{Z} \right\}$

ولتكن I مجموعة جزئية من R تتكون من المصفوفات ذات المداخل (العناصر) التى هى أعداد زوجية. يترك للقارئ البرهنة على أن I مثالى فى R .

المطلوب حساب عدد عناصر الحلقة

$$R/I := \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + I \mid a_i \in \mathbb{Z} \right\}$$

الحل : سنكتب

$$a_i = \begin{cases} 1 + (a_i - 1) & , \quad a_i \ \text{فردى} \\ & , i = 1, \ldots, 4 \\ 0 + a_i & , \quad a_i \ \text{زوجى} \end{cases}$$

وبالتالى يكون أى عنصر فى R/I على الشكل :

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + I = \begin{bmatrix} 1 \text{ or } 0 & 1 \text{ or } 0 \\ 1 \text{ or } 0 & 1 \text{ or } 0 \end{bmatrix} + \begin{bmatrix} 2x & 2y \\ 2z & 2w \end{bmatrix} + I; x, y, z, w \in \mathbb{Z}$$

$$= \begin{bmatrix} 1 \text{ or } 0 & 1 \text{ or } 0 \\ 1 \text{ or } 0 & 1 \text{ or } 0 \end{bmatrix} + I$$

لأن $\begin{bmatrix} 2x & 2y \\ 2z & 2w \end{bmatrix} \in I$

ومن ثم يكون عدد عناصر الحلقة R/I هو 2^4 أى 16 .

مثال٣ : فى النظرية (١-٣-١) رأينا أن الشرط $A \subset R$ مثالى كاف حتى يمكن تكوين الحلقة R/A. برهن على أنه ضرورى كذلك .

البرهان : ليكن A ليس مثالياً فى R (ليكن حلقة جزئية فى R) . إذن يوجد $r \in R$ ، $a \in A$ بحيث يكون $ra \notin A$ أو $ar \notin A$. ليكن $ra \notin A$ مثلاً . والآن :

$$0 + A = A = a + A \qquad (\text{لأن } a \in A)$$

ولكن

$$(r + A)(a + A) = ra + A \neq A \quad (\text{لأن } ra \notin A)$$

بينما $(r + A)(0 + A) = r0 + A = A$

إذن عملية الضرب فى "الحلقة" R/A ليست معرفة وبالتالى فإن R/A ليست حلقة .

(قارن مع ملحوظة (١-٣-٢))

مثال ٤:برهن على أن الحلقة R/N حيث N مثالى فى R تكون إبدالية إذا كان وفقط إذا كان:

$\forall r, s \in R : (rs - sr) \in N$

البرهان :

$$R/N \text{ إبدالية } \Leftrightarrow \forall r, s \in R : (r + N)(s + N) = (s + N)(r + N)$$

$$\Leftrightarrow \forall r,s \in R : rs + N = sr + N \Leftrightarrow rs - sr \in N$$

مثال٥ : برهن على أنه إذا كانت R حلقة بها عنصر الوحدة ، وكان N مثالياً فى R ، بحيث إن $N \neq R$ ، فإن R/N حلقة لها عنصر الوحدة $\neq$ الصفر .

البرهان : نعلم أن R/N حلقة ، وكذلك إذا كان $1 \in R$ هو عنصر الوحدة ، فإن $1 + N$ هو عنصر الوحدة فى R/N . صفر الحلقة R/N هو N . المطلوب إثبات أن $1 + N \neq N$.

ولكن $1 + N = N$ يعنى أن $1 \in N$ وإذا كان $1 \in N$ فإن $N = R$ (انظر مثال ٢٥ فى (١-٢-٨)) ، وهذا تناقض . أى أن $1 + N \neq N$

مثال٦ : برهن على أن الحلقة العاملة لحقل إما أن تكون الحلقة التافهة ذات العنصر الواحد أو أن تكون متشاكلة مع الحقل نفسه .

البرهان : ليكن F حقلاً وليكن A مثالياً فى الحقل F . نعلم من مثال٢٥ (١-٢-٨) أن A إما أن يساوى الحقل نفسه ، أى أن $A = F$ أو أن $A = \{0\}$. وبهذا تكون الحلقة العاملة F/A إما F/F وتكون فى هذه الحالة

$$F/F = \{x + F \mid x \in F\} = \{F\}$$

أى حلقة ذات عنصر واحد هو F أو

$$F/\{0\} = \{x + \{0\} \mid x \in F\} \cong F$$

$$x + \{0\} \leftrightarrow x$$

مثال ٧ : برهن على مجموعة العناصر منعدمة القوة (nilpotent) فى حلقة إبدالية تكون مثالياً (انظر مثال١٢ فى (١-١-١٥))

البرهان : بدهى أن 0 عنصر منعدم القوة فى الحلقة ، إذن مجموعة العناصر منعدمة القوة ليست خالية .

ليكن a ، b عنصرين منعدمى القوة ، أى أنه يوجد m ، n عددين صحيحين موجبين بحيث إن $a^m = 0$ ، $b^n = 0$. والآن نعرف $k := m + n$

$$(a-b)^k=(a-b)^{m+n}=a^{m+n}+\binom{m+n}{1}a^{m+n-1}(-b)+\ldots+\binom{m+n}{r}a^{m+n-r}(-b)^r+\ldots$$
$$+\binom{m+n}{m+n-1}a(-b)^{m+n-1}+(-b)^{m+n}$$

الحد العام فى المفكوك هو $\binom{m+n}{r}a^{m+n-r}b^r$ وهو يساوى الصفر ، لأنه إذا كان $r\le n$

فإن $a^{m+n-r}=0$ ، وإذا كان $r\ge n$ فإن $(-b)^r=0$

وبالتالى فإنه يوجد عدد صحيح موجب $k=m+n$ بحيث إن $(a-b)^k=0$، أى أن $a-b$ عنصر منعدم القوة .

كذلك إذا كان a كما سبق عنصراً منعدم القوة أى أنه يوجد m عدد صحيح موجب بحيث إن $a^m=0$ ، فإنه لأى $r\in R$ يكون $(ra)^m = r^m a^m = r^m 0=0$. أى أن ra عنصر منعدم القوة . والآن R إبدالية

R إبدالية يستلزم أن ar عنصر منعدم القوة كذلك . ومن ثم البرهان .

تسمى مجموعة العناصر منعدمة القوة فى حلقة إبدالية R "جذر R" (The radical of R) .

مثال٨ : اوجد جميع المثاليات N فى الحلقة $\mathbb{Z}/12\mathbb{Z}$ ، واحسب فى كل مرة $\dfrac{\mathbb{Z}/12\mathbb{Z}}{N}$.

الحل : المثاليات فى $\mathbb{Z}/12\mathbb{Z}$ هى : المثالى التافه أولاً $\{0\}/12\mathbb{Z}$ ويكون $\dfrac{\mathbb{Z}/12\mathbb{Z}}{\{0\}/12\mathbb{Z}}\cong\mathbb{Z}/\{0\}\cong\mathbb{Z}$ ، ثانياً : $2\mathbb{Z}/12\mathbb{Z}$ ، ويكون $\dfrac{\mathbb{Z}/12\mathbb{Z}}{2\mathbb{Z}/12\mathbb{Z}}\cong\mathbb{Z}/2\mathbb{Z}$ ،

$x+\{0\}\leftrightarrow x$ ٥-٣-١

وثالثاً : $3\mathbb{Z}/12\mathbb{Z}$ ، ويكون $\dfrac{\mathbb{Z}/12\mathbb{Z}}{3\mathbb{Z}/12\mathbb{Z}}\cong\mathbb{Z}/3\mathbb{Z}$ ، رابعاً : $4\mathbb{Z}/12\mathbb{Z}$

٥-٣-١

ويكون $\dfrac{\mathbb{Z}/12\mathbb{Z}}{4\mathbb{Z}/12\mathbb{Z}}\cong\mathbb{Z}/4\mathbb{Z}$ ، خامساً : $6\mathbb{Z}/12\mathbb{Z}$ ويكون $\dfrac{\mathbb{Z}/12\mathbb{Z}}{6\mathbb{Z}/12\mathbb{Z}}\cong\mathbb{Z}/6\mathbb{Z}$ ،

وسادساً: المثالى التافه $\mathbb{Z}/12\mathbb{Z}$ ، ويكون $\{\bar{0}\}=\{\mathbb{Z}/12\mathbb{Z}\} \cong \dfrac{\mathbb{Z}/12\mathbb{Z}}{\mathbb{Z}/12\mathbb{Z}}$ ($\bar{0}$ هو صفر الحلقة $\mathbb{Z}/12\mathbb{Z}$ أى هو $\dfrac{\mathbb{Z}/12\mathbb{Z}}{\mathbb{Z}/12\mathbb{Z}}$)

مثال ٩ : بالإشارة إلى مثال ٧ السابق اوجد جذر الحلقة $\mathbb{Z}/12\mathbb{Z}$ ، الحلقة $\mathbb{Z}$

الحل : $z+12\mathbb{Z}$ يقع فى جذر $\mathbb{Z}/12\mathbb{Z}$ إذا وجد عدد صحيح موجب n بحيث يكون $(z+12\mathbb{Z})^n = 12\mathbb{Z}$ ($12\mathbb{Z}$ هو صفر الحلقة $\mathbb{Z}/12\mathbb{Z}$)

$$\Rightarrow z^n + 12\mathbb{Z} = 12\mathbb{Z} \Rightarrow z^n \in 12\mathbb{Z} = \{0, \pm 12, \pm 24, \pm 36, \ldots\}$$
$$\Rightarrow z \in \{0, \pm 6, \pm 12, \ldots\}$$

ويكون جذر $\mathbb{Z}/12\mathbb{Z}$ هو $\{0+12\mathbb{Z}, 6+12\mathbb{Z}\}$ أى هو $\{\bar{0}, \bar{6}\}$.

لاحظ أن هذا الجزء هو المثالى $6\mathbb{Z}/12\mathbb{Z}$ كذلك لاحظ أن $\pm 12 + 12\mathbb{Z} = 12\mathbb{Z}$ ، $-6+12\mathbb{Z} = 6+12\mathbb{Z}$.

z يقع فى جذر $\mathbb{Z}$ إذا وجد عدد صحيح موجب n بحيث يكون $z^n = 0$ وهذا يحدث إذا كان وفقط إذا كان $z = 0$ أى أن جذر $\mathbb{Z}$ هو $\{0\}$.

مثال ١٠ : يترك للقارئ التحقق من أن $N = \{\bar{0}, \bar{3}\}$ مثالى فى $\mathbb{Z}/6\mathbb{Z}$. اوجد $\dfrac{\mathbb{Z}/6\mathbb{Z}}{N}$

الحـل :

$$N = \{0+6\mathbb{Z}, 3+6\mathbb{Z}\} = 3\mathbb{Z}/6\mathbb{Z}$$

وبالتالى فإن :

$$\dfrac{\mathbb{Z}/6\mathbb{Z}}{3\mathbb{Z}/6\mathbb{Z}} \cong \mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$$

١-٣-٥

مثال ١١ : إذا كانت N هى جذر حلقة إبدالية R فبرهن على أن المثالى التافه $\{N\}$ هو جذر R/N

البرهان : سنشير إلى جذر R بأنه $Rad(R)$. والآن :

$$Rad(R/N) = \{x+N \mid (x+N)^n = N, x \in R, \quad n \in \mathbb{N} \text{ لبعض } \}$$

$$= \{x+N \mid x^n + N = N, x \in R, \quad n \in \mathbb{N} \text{ لبعض } \}$$

$$= \{x+N \mid x^n \in N, x \in R, \quad n \in \mathbb{N} \text{ لبعض } \}$$

$$= \{x+N \mid x^{nm} = (x^n)^m = 0, x \in R, \quad n,m \in \mathbb{N} \text{ لبعض } \}$$

$$N = Rad(R)$$

$$= \{x+N \mid x \in Rad(R) = N\} = \{N\}$$

مثال ١٢ : لتكن R حلقة إبدالية ، N مثالى فى R ، برهن على أن المجموعة $\sqrt{N}$ المعرفة كالآتى :

$$\sqrt{N} := \{a \in R \mid a^n \in N \quad n \in \mathbb{N} \text{ لبعض } \}$$

مثالى فى R . تسمى هذه المجموعة "جذر N" $(Rad(N))$

البرهان : واضح أن $0 \in \sqrt{N}$ أى أن $\sqrt{N}$ ليس مجموعة خالية . والآن :

$$\forall a \in \sqrt{N} \;\; \forall r \in R \Rightarrow a^n \in N, r^n \in R \Rightarrow (ra)^n \underset{\text{إبدالية } R}{=} r^n a^n \in N$$

$$\Rightarrow ra \in \sqrt{N} \underset{\text{إبدالية } R}{\Rightarrow} ar \in \sqrt{N}$$

$$a,b \in \sqrt{N} \Rightarrow \exists m,n \in \mathbb{N} : a^m \in N, b^m \in N \Rightarrow$$

$$(a-b)^{m+n} = a^{m+n} + \binom{m+n}{1} a^{m+n-1}(-b) + \ldots + \binom{m+n}{r} a^{m+n-r}(-b)^r + \ldots$$

$$+ \binom{m+n}{1} a(-b)^{m+n-1} + (-b)^{m+n}$$

الحد العام هو : $T_r = \binom{m+n}{r} d^{m+n-r}(-b)^r$. كما فى مثال ٦ إذا كان $r \le n$ فإن $d^{m+n-r} \in N$

ويكون $T_r \in \sqrt{N}$ (N مثالى) . وإذا كان $n \le r$ يكون $T_r \in \sqrt{N}$ (N مثالى) . ومن ثم

فإن $(a-b)^{m+n} \in N$ ويكون $a-b \in \sqrt{N}$.

نهاية البرهان .

<u>مثال ١٣</u> : هل تعريفا "الجذر" الواردان فى مثالى ٧ ، ١٢ متسقان consistent ؟

<u>الحل</u> : من مثال ١٢ يتضح أن :

$$a \in R \Rightarrow a^n \in R \quad n \in \mathbb{N} \text{ لبعض } \Rightarrow a \in \sqrt{R} \Rightarrow R \subset \sqrt{R}$$

لكن $\sqrt{R} \subset R$ ومن ثم فإن $\sqrt{R} = R$ (جذر R)

أما في مثال ٧ فإن $\sqrt{R}$ ليس دائماً مساوياً لـــ R

إذن التعريفان غير متسقين (inconsistent) .

<u>مثال ١٤</u> : ما العلاقة بين المثالى $\sqrt{N}$ فى مثال ١٢ ، والجذر $Rad(R/N)$ فى مثال ٧ ؟

<u>الحل</u> : سنبرهن على أن $Rad(R/N) = \sqrt{N}/N$

$$\bar{x}(=x+N) \in Rad(R/N) \Leftrightarrow (\bar{x})^n = N \quad (R/N \text{ العنصر الصفرى فى}) \; n \in \mathbb{N} \text{ لبعض } \Leftrightarrow$$

$$\Leftrightarrow (\overline{x^n}) = N,\; n \in \mathbb{N} \text{ لبعض } \Leftrightarrow x^n \in N ,n \in \mathbb{N} \text{ لبعض } \Leftrightarrow x \in \sqrt{N} \Leftrightarrow \bar{x} \in \sqrt{N}/N$$

<u>مثال١٥</u> : ليكن A ، B مثاليين فى الحلقة الإبدالية R . تعرف القسمة A على B $(A:B)$

(The quotient of A by B)

بأنها $\quad A:B := \{r \in R \,|\, rb \in A \quad \forall b \in B\}$

برهن على أن $A:B$ مثالى فى الحلقة R .

البرهان : واضح أن $0 \in A:B$ ، أى أن $A:B \ne \phi$

$$r,s \in A:B \Rightarrow \forall b \in B \quad rb, sb \in A \Rightarrow \forall b \in B \quad (r-s)b = rb - sb \in A$$

A مثالى

$\Rightarrow r-s\in A:B$

$r\in A:B,\lambda\in R\Rightarrow \forall b\in B\ \ rb\in A,\lambda\in R\Rightarrow \forall b\in B:(\lambda r)b=\lambda(rb)\ \in\ A$

A مثالى

البرهان $\Rightarrow$ $\Rightarrow \lambda r\in A:B$

١-٣-٧ تعريف : لتكن R حلقة . يقال لمثالى $P\subset R$ إنه مثالى أولى (prime ideal) إذا كان :

(1) $P\neq R$

(2) $\forall a,b\in R: ab\in P\Rightarrow a\in P$ أو $b\in P$

بعبارة أخرى تكافىء العبارة (2) :

$a\in R\setminus P$ و $b\in R\setminus P\Rightarrow ab\in R\setminus P$

١-٣-٨ أمثلة :

(١) $m\in\mathbb{N}$ $(m\neq 0)$ يقتضى أن $m\mathbb{Z}$ مثالى أولى فى $\mathbb{Z}$ إذا كان وفقط إذا كان m عدداً أولياً. (راجع (١-٢-٧ (٣))

البرهان : "$\Rightarrow$" : ليكن m عدداً أولياً وليكن $k\ell\in m\mathbb{Z}\neq\mathbb{Z}$. هذا يستلزم أنه يوجد $z\in\mathbb{Z}$ بحيث يكون $k\ell=mz$. أى أن m قاسم لـــ $k\ell$. ولأن m عدد أولى إذن m يقسم k أو يقسم ℓ. أى أنه يوجد $x,y\in\mathbb{Z}$ بحيث يكون $k=x\,m$ أو $\ell=ym$ وهذا يقتضى أن $k\in m\mathbb{Z}$ أو $\ell\in m\mathbb{Z}$.

"$\Leftarrow$" : إذا كان m ليس عدداً أولياً ، فإنه يوجد عددان ℓ,k بحيث يكون $m=k\ell$ ، $1<k,\ell<m$. ولكن $k\ell=m\in m\mathbb{Z}$ بينما $k,\ell\notin m\mathbb{Z}$

(٢) المثالى $\{0\}\subset\mathbb{Z}$ أولى

١-٣-٩ نظرية :

لتكن R حلقة إبدالية ، لها عنصر الوحدة "1" ، وليكن P مثالياً فى R . التقريرات الآتية متكافئة :

(١) P مثالى أولى

(٢) الحلقة R/P نطاق متكامل

(٣) يوجد نطاق متكامل R'، ويوجد هومومورفيزم حلق $\varphi:R\to R'$ بحيث يكون $Ker(\varphi)=P$

<u>البرهان</u> : (١)⇐ (٢) : لأن R حلقة إبدالية لها عنصر الوحدة 1 ، فإن R/P يكون حلقة إبدالية لها عنصر الوحدة $1+P$. P هو صفر الحلقة R/P حيث $1+P\neq P$ ، وإلا فإن $1\in P$ وبالتالى يكون $P=R$ وهذا تناقض مع كون P مثالياً أولياً . يتبقى أن نثبت أن R/P خالية من القواسم الصفرية أى أنه إذا كان $(a+P)(b+P)=P$ فإن $a+P=P$ أو $b+P=P$.
$(a+P)(b+P)=P$ يعنى أن $ab+P=P$ أى أن $ab\in P$. ومن حيث أن P مثالى أولى فإن $a\in P$ أو $b\in P$ وبالتالى يكون $a+P=P$ أو $b+P=P$.

(٢)⇐(٣): نعرف $R':=R/P$ ، $\rho:R\to R/P$ الإبيمورفيزم الطبيعى، ويكون $Ker(\rho)=P$

(٣) ⇐ (١) : $R'=R/P$ نطاق متكامل يستلزم أن $1+P\neq P$ أى أن $1\notin P$ وبالتالى فإن $P\neq R$

ليكن $a,b\in R$ بحيث إن $ab\in P=Ker(\varphi)$. هذا يقتضى أن $\varphi(a)\varphi(b)=\varphi(ab)=0$.
من حيث أن R' نطاق متكامل ينتج أن $\varphi(a)=0$ أو $\varphi(b)=0$ وبالتالى فإن $a\in Ker(\varphi)=P$ أو $b\in Ker(\varphi)=P$.

نهاية البرهان .

<u>١-٣-١٠ تعريف</u> :

لتكن R حلقة . يقال لمثالى $M\subset R$ إنه مثالى أعظم (maximal ideal) إذا كان :

(١) $M\neq R$

(٢) لايوجد مثالى $A\subset R$ بحيث يكون $M\subsetneq A\subsetneq R$

(هذا لايعنى أنه لجميع المثاليات $A\subsetneq R$ يكون : $A\subset M$)

١-٣-١١ نظرية :

لتكن R حلقة إبدالية ذات عنصر الوحدة "1" . وليكن $A \subset R$ مثالى .

$$R/A \text{ حقل } \Leftrightarrow A \text{ مثالى اعظم}$$

البرهان : "$\Leftarrow$" : R/A حقل يستلزم أن $A \neq 1+A$ أى أن $1 \notin A$ وبالتالى فإن $A \neq R$

والآن ليكن $B \subset R$ مثالياً يحتوى على A فعلياً ، أى أن $A \subsetneq B$. إذن يوجد b بحيث إن $b \notin A$ ، $b \in B$. عندئذ فإن $b + A$ يكون عنصراً غير صفرى (أى ليس مساوياً للصفر) فى R/A (صفر R/A هو A كما نعلم) ، وبالتالى فإنه يوجد $c + A$ بحيث يكون $(b+A)(c+A)=1+A$ ($1+A$ هو عنصر الوحدة فى R/A كما سبق) . أى أن :

$$1+A=(b+A)(c+A)=bc+A$$

وهذا يقتضى أن $1-bc \in A \subset B$. ولكن $b \in B$ يستلزم أن $bc \in B$ ومن ثم فإن :

$$1=1-bc+bc \in B \qquad (\text{لأن } B \text{ مثالى})$$

وهذا يستلزم أن $B = R$. أى أن A مثالى أعظم .

"$\Rightarrow$" : $A \subsetneq R$ مثالى أعظم يستلزم أن $1 \notin A$ أى أن $1+A \neq A$ (أى أن صفر R/A لا يساوى عنصر الوحدة $1+A$ فيه) . R حلقة إبدالية يستلزم أن R/A حلقة إبدالية .

والآن ليكن $b \in R$ ، $b \notin A$. يتبقى أن نثبت أن $b+A$ لها معكوس ضربى .

نعرف :

$$B := \{br + a \mid r \in R, a \in A\}$$

يسهل التحقق من أن B مثالى يحتوى على A فعلياً (بأخذ $r = 0$) .

ولأن A مثالى أعظم فإن $B = R$. وبالتالى فإن $1 \in B$ وبهذا فإنه يوجد $c \in R$ ، $a' \in A$ بحيث يكون $1=bc+a'$. والآن :

$$1+A=bc+a'+A \underset{a' \in A \text{ مثالى}}{=} bc+A=(b+A)(c+A)$$

أى أن $b+A$ له معكوس ضربى . نهاية البرهان .

١-٣-١٢ أمثلة :

(١) فى الحقل K يكون المثالى $\{0\}$ مثالياً أعظم لأنه لايوجد فى أى حقل سوى مثاليين الحقل نفسه أو المثالى $\{0\}$. (مثال ٢٥ فى (١-٢-٨)). المثالى K ليس مثالياً أعظم بالتعريف .

(٢) فى الحلقة $\mathbb{Z}$ جميع المثاليات الأولية فيما عدا $\{0\}$ مثاليات عظمى .
من (١-٢-٧) نعلم أن جميع المثاليات فى $\mathbb{Z}$ تكون على الصورة $m\mathbb{Z}$ حيث $m\in\mathbb{Z}$
ومن(١-٣-٨) نعلم أن $m\mathbb{Z}$ مثالى أولى إذا كان وفقط إذا كان m عدداً أولياً أو $m=0$.
أى أن P مثالى أولى فى $\mathbb{Z}$ إذا كان وفقط إذا كان p عدداً أولياً بحيث يكون $P=p\mathbb{Z}$ أو $P=\{0\}$. والآن من (١-٣-٩) P مثالى أولى إذا كان وفقط إذا كان $\mathbb{Z}/p\mathbb{Z}$ نطاقاً متكاملاً أو $\mathbb{Z}/\{0\}$ نطاقاً متكاملاً . ولكن $\mathbb{Z}/p\mathbb{Z}$ نطاق متكامل منته ، ومن (١-١-١٣) يكون $\mathbb{Z}/p\mathbb{Z}$ حقلاً ، ومن (١-٣-١١) يكون $p\mathbb{Z}$ مثالياً أعظم فى $\mathbb{Z}$.

(٣) كل مثالى A فى $\mathbb{Z}$ ، $A\neq\mathbb{Z}$ يكون محتوىً فى مثالى أعظم فى $\mathbb{Z}$.
مرة أخرى نعلم أن A مثالى فى $\mathbb{Z}$ إذا كان $A=m\mathbb{Z}$ حيث m عدد طبيعى (أو $m=0$).
فى حالة $m=0$ واضح أن A يكون محتوى فى مثالى أعظم (لأن أى مثالى فى $\mathbb{Z}$ يحتوى على العنصر 0). إذا كان $m\geq 2$ (الحالة $m=1$ مستبعدة لأن $A\neq\mathbb{Z}$) فإنه يوجد قاسم لـــ m هو p حيث p عدد أولى ونحصل على $A=m\mathbb{Z}\subset p\mathbb{Z}$. ومن مثال٢ السابق مباشرة $p\mathbb{Z}$ هو مثالى أعظم .

١-٣-١٣ تعريف :

لتكن M مجموعة . ولتكن $H\subset M\times M$. يقال إن H **ترتيب جزئى** (partial order) فى M إذا تحقق :

(أ) لكل $a\in M$: $(a,a)\in H$

(ب) $(a,b)\in H$ ، $(b,a)\in H$ يستلزم أن $a=b$

(جـ) $(a,b)\in H$ ، $(b,c)\in H$ يستلزم أن $(a,c)\in H$

غالباً ما نكتب $a\leq b$ للتعبير عن $(a,b)\in H$ ، وتستخدم"$\leq$" للتعبير عن الترتيب الجزئى .

<u>١-٣-١٤ تعريف</u> :

(أ) لتكن M مجموعة ، وليكن "$\leq$" ترتيباً جزئياً فى M . يقال أن "$\leq$" <u>ترتيب كلى</u> فى M (total order) إذا كان لكل عنصرين $a,b\in M$ يكون $a\leq b$ أو $b\leq a$

(ب) إذا كان "$\leq$" ترتيباً جزئياً فى مجموعة M . تسمى المجموعة الجزئية غير الخالية K من M <u>سلسلة</u> (chain) فى M (بالنسبة إلى "$\leq$") إذا كان لكل عنصرين $a,b\in K$ يكون : $a\leq b$ أو $b\leq a$.

<u>١-٣-١٥ أمثلة</u> :

(١) العلاقة المعتادة "أقل من أو يساوى" على $\mathbb{R}$ هى ترتيب كلى فى $\mathbb{R}$.

(٢) إذا كانت M مجموعة فيكون $A\leq B :\Leftrightarrow A\subset B$ ترتيباً جزئياً لمجموعة القوة $\mathbb{P}(M)$ لـ M

وإذا كان $M:=\{a,b\}$ ، $a\neq b$ فإن الترتيب الجزئى ليس ترتيباً كلياً ، لأنه لايحدث $\{a\}\leq\{b\}$ ولايحدث $\{b\}\leq\{a\}$.

<u>١-٣-١٦ تعريف</u> :

لتكن M زمرة ، "$\leq$" ترتيباً جزئياً ، A مجموعة جزئية من M .

(أ) يقال لعنصر $s\in M$ إنه <u>حد أعلى</u> (upper bound) أو <u>حد أدنى</u> (lower bound) فى A إذا كان $a\leq s$ أو $s\leq a$ على الترتيب لجميع $a\in A$.

(ب) يقال لعنصر $a\in A$ إنه <u>عنصر أخير</u> (last lement) إذا كان a حداً أعلى فى A . ويقال إنه <u>عنصر أول</u> (first element) إذا كان a حداً أدنى فى A .

(جـ) يقال لعنصر $m\in A$ إنه <u>عنصر أعظم</u>(maximal element) فى A أو <u>عنصر أصغر</u> (minimal element) فى A إذا كان لكل a عنصر فى A : $m\leq a$ أو $a\leq m$ على الترتيب ينتج أن $m=a$.

١-٣-١٧ ملحوظة :

لتكن M مجموعة ، وليكن "$\leq$" ترتيباً جزئياً ، A مجموعة جزئية من M .

(أ) A لها على الأكثر عنصر أخير واحد وعلى الأكثر عنصر أول واحد .

(ب) إذا كان لـــ A عنصر أخير a (أو عنصر أول a) فإن لـــ A عنصر أعظم واحد بالضبط هو a (أو عنصر أصغر واحد بالضبط) هو a .

(جـــ) ليكن V فراغاً خطياً (vector space) ذا بعد ($\dim V > 1$) $1 <$ ولتكن A مجموعة جميع الفراغات الخطية الجزئية U (vector subspaces) فى V ، حيث بعد $U \geq 1$ ($\dim U \geq 1$) . عندئذ فإنه من خلال التعريف $U \subset W \;:\Leftrightarrow\; U \leq W$ يوضح ترتيب جزئى "$\leq$" فى A . ولأن $\dim V > 1$ لايكون هناك عنصر أول لـــ A . بينما كل فراغ جزئى من V ذى بعد 1 سيكون عنصراً أصغر فى A .

١-٣-١٨ تعريف :

لتكن M مجموعة غير خالية . وليكن "$\leq$" ترتيباً جزئياً فى M . يقال إن M **مرتبة استقرائياً** (inductively ordered) لـــ "$\leq$" إذا كانت كل سلسلة فى M لها حد أعلى .

١-٣-١٩ بدهية زورن Zorn's Lemma

كل مجموعة مرتبة إستقرائياً لها على الأقل عنصر أعظم

من المعلوم أن بدهية زورن تكافئ بدهية الاختيار (Axiom of choice) التى تنص على أن "حاصل الضرب الكارتيزى لعائلة غير خالية من المجموعات غير الخالية ليس خالياً"

"The Cartesian product of a non-empty family of non-empty sets is non-empty"

وفى حلقة نويترية (سنعرفها فيما بعد) R لاتساوى $\{0\}$ لكل مثالى A يوجد مثالى أعظم M بحيث إن $A \subset M$. ومجموعة كل المثاليات فى R والتى لاتساوى R والتى تحتوى على A لها مثالى أعظم . وهذا المثالى الأعظم مثالى أعظم فى R . وباستخدام بدهية زورن سنبرهن على أن هناك موقفاً مشابهاً لكل حلقة إبدالية لها عنصر وحدة يختلف عن صفرها .

١-٣-٢٠ نظرية :

لتكن R حلقة إبدالية ، لها عنصر الوحدة غير مساو لصفرها . عندئذ فإنه لكل مثالى $A \subsetneq R$ يوجد مثالى أعظم M فى R بحيث إن $A \subset M$.

البرهان : لتكن I مجموعة كل المثاليات B فى R بحيث إن $A \subset B \subsetneq R$. سنعرف ترتيباً جزئياً "$\leq$" فى I كالآتى : $B \leq C :\Leftrightarrow B \subset C$. وبهذا تكون I مرتبة استقرائياً من خلال "$\leq$" لأن : $A \in I$ يجعل I غير خالية ، وإذا كانت K سلسلة فى I فإن $\bigcup_{B \in K} B$ يكون عنصراً فى I لأن : $\bigcup_{B \in K} B$ مثالى فى R ، لأن $K \neq \phi$ يستلزم أن $\bigcup_{B \in K} B \neq \phi$. وكذلك $b, c \in \bigcup_{B \in K} B$ يقتضى أنه يوجد $C, D \in K$ بحيث إن $b \in C$ ، $c \in D$. ولأن K سلسلة فإن $C \subset D$ أو $D \subset C$ ، وبالتالى يكون $b - c \in C$ أو $b - c \in D$ أى أن $b - c \in \bigcup_{B \in K} B$. وأيضاً $b \in \bigcup_{B \in K} B$ يقتضى أن $rb \in \bigcup_{B \in K} B$ لجميع $r \in R$ والآن $A \subset \bigcup_{B \in K} B \subsetneq R$ ، لأنه إذا كان $\bigcup_{B \in K} B = R$ فإن عنصر الوحدة 1 فى R يجب أن ينتمى إلى C – مثلاً – أحد عناصر K . وبهذا يكون $C = R$. وهذا تناقض . والآن من بدهية زورن يجب أن تحتوى I على عنصر أعظم M ، الذى هو – كما هو واضح – مثالى أعظم فى R بحيث إن $A \subset M$. ∎

١-٣-٢٠ أمثلة محلولة :

مثال ١ : ليكن $\varphi : R \to R'$ هومومورفيزم حلق بحيث إن $\varphi(1) = 1'$ ($1', 1$ عنصرا الوحدة فى R، R' على الترتيب) . وليكن A' مثالياً أولياً فى R' .

برهن على أن $\varphi^{-1}(A')$ مثالى أولى فى R .

البرهان : نعلم أن $\varphi^{-1}(A')$ مثالى من مثال ١١ فى (١-٢-٨). يتبقى أن نثبت أنه أولى . $\varphi^{-1}(A') \neq R$ ، لأنه إذا كان $\varphi^{-1}(A') = R$ فإن $1 \in \varphi^{-1}(A')$ وبالتالى فإن $1' = \varphi(1) \in A'$ وهذا يقتضى $A' = R$: تناقض لأن A' مثالى أولى فى R' .

ليكن $xy \in \varphi^{-1}(A')$. هذا يستلزم أن $\varphi(x)\varphi(y) = \varphi(xy) \in A'$. لأن A' مثالى أولى فإن $\varphi(x) \in A'$ أو $\varphi(y) \in A'$ وبالتالى فإن $x \in \varphi^{-1}(A')$ أو $y \in \varphi^{-1}(A')$.

مثال ٢ : أوجد جميع المثاليات الأولية والعظمى فى $\mathbb{Z}/12\mathbb{Z}$.

الحل : انظر مثال ٨ فى (١-٣-٦). المثالى $\{0\}/12\mathbb{Z}$ مثالى أولى ، لكنه ليس مثاليا أعظم.

اعتبر المثالى $2\mathbb{Z}/12\mathbb{Z}$. $\dfrac{\mathbb{Z}/12\mathbb{Z}}{2\mathbb{Z}/12\mathbb{Z}}$ حلقة تشاكل الحلقة $\mathbb{Z}/2\mathbb{Z}$ من (١-٣-٥)

وهذه نطاق متكامل من (١-٣-٨) ، (١-٣-٩) . ومن (١-١-١٣) هى حقل . ومن (١-٣-١١) يكون $2\mathbb{Z}/12\mathbb{Z}$ مثاليا أعظم وبالتالى فهو أولى (لماذا) ؟ كذلك اعتبر المثالى

$3\mathbb{Z}/12\mathbb{Z}$. الحلقة $\dfrac{\mathbb{Z}/12\mathbb{Z}}{3\mathbb{Z}/12\mathbb{Z}}$ تشاكل الحلقة $\mathbb{Z}/3\mathbb{Z}$ وبتسلسل مشابه تماماً لما

سبق يكون $3\mathbb{Z}/12\mathbb{Z}$ مثالياً أعظم ومثالياً أولياً فى $\mathbb{Z}/12\mathbb{Z}$. لماذا لاتوجد مثاليات أولية أو عظمى أخرى ؟

مثال ٣ : ليكن K حقلاً . وليكن $\varphi : K \to K$ هومومورفيزم حلق . برهن على أن φ إما أن يكون الراسم الصفرى (أى أن $\varphi(K) = \{0\}$) أو أن φ أيزومورفيزم .

البرهان : فى مثال ٣٣ من (١-٢-٨) رأينا أن $Ker(\varphi) = \{0\}$ أو $Ker(\varphi) = K$. ومن (١-٣-٣) ينتج أن :

$$Ker(\varphi) = \{0\} \Rightarrow K/\{0\} \cong \varphi(K)$$

أى أن $K \cong \varphi(K)$ أى أن φ أيزومورفيزم

(لاحظ أن $\begin{array}{c} K \cong K/\{0\} \\ x \leftrightarrow x + \{0\} \end{array}$)

$$Ker(\varphi) = K \Rightarrow K/K \cong \varphi(K)$$

أى أن $\varphi(K) \cong \{\overline{0}\}$ ، أى أن φ هو الراسم الصفرى .

(وبالطبع ينتج مباشرة من $Ker(\varphi) = K$ أن φ هو الراسم الصفرى)

مثال ٤ : ليكن $S := \{a+bi \mid a,b \in \mathbb{Z}, b$ عدد زوجى $\}$. برهن على أن S حلقة جزئية من $\mathbb{Z}[i]$ ، لكن S ليست مثاليا فى $\mathbb{Z}[i]$.

البرهان : $0+0i \in S$. أى أن $S \neq \phi$.

$a+2bi, c+2di \in S$ حيث $a,b,c,d \in \mathbb{Z}$ ينتج أن :

$$a+2bi-(c+2di) = a-c+2(b-d)i \in S,$$

$(a+2bi)(c+2di) = ac-4bd+2(ad+bc)i \in S$. وينتج أن S حلقة جزئية من $\mathbb{Z}[i]$.

ليكن $1+2i \in S$ ، $1-i \in \mathbb{Z}[i]$:

$(1-i)(1+2i) = 3+i \notin S \Rightarrow$ S ليست مثاليا فى $\mathbb{Z}[i]$

مثال ٥ : برهن على أن المثالى $[X^2+1]$ (أى المثالى المتولد من العنصر X^2+1) فى $\mathbb{R}[X]$ (حلقة كثيرات الحدود ذات المعاملات الحقيقية) مثالى أعظم

البرهان : نعتبر الراسم :

$$\varphi : \mathbb{R}[X] \to \mathbb{C}$$
$$f \mapsto f(i)$$

(أى أن $\varphi(f) = f(i)$) . هذا الراسم شامل (غامر ، فوقى) وهذا واضح . وكذلك هو هومومورفيزم حلقى لأن :

$$\forall f, g \in \mathbb{R}[X] : \varphi(f+g) = (f+g)(i) = f(i) + g(i) = \varphi(f) + \varphi(g),$$
$$\varphi(f.g) = (f.g)(i) = f(i).g(i) = \varphi(f).\varphi(g)$$

ونبرهن على أن نواة (φ) هى :

$$Ker(\varphi) = [X^2+1]$$

واضح أن $Ker(\varphi)$ $[X^2+1]\subset Ker(\varphi)$ (لأن $i^2+1=0$) . والآن نبرهن على أن $Ker(\varphi)\subset[X^2+1]$:

ليكن $f\in Ker(\varphi)$. هذا يستلزم أنه يوجد $q,r\in\mathbb{R}[X]$ بحيث إن $f=q(X^2+1)+r$ ،
r من الدرجة الأولى (سندرس هذا بالتفصيل فيما بعد) . أى أنه يوجد $a,b\in\mathbb{R}$ بحيث
أن $r=aX+b$. والآن :

$$0\underset{f\in Ker(\varphi)}{=}f(i)=ai+b\Rightarrow a=0,b=0$$

أى أن $f=q(X^2+1)\in[X^2+1]$ أى أن $Ker(\varphi)\subset[X^2+1]$ ، ومن ثم فإن

$$Ker(\varphi)=[X^2+1]$$

والآن نطبق النظرية (١-٣-٣) (نظرية الهومومورفيزم) فنحصل على :

$$\mathbb{R}[X]/[X^2+1]=\mathbb{R}[X]/Ker(\varphi)\cong\varphi(\mathbb{R}[X])\underset{\varphi\text{ غامر}}{=}\mathbb{C}$$

ومن حيث إن $\mathbb{R}[X]$ حلقة إبدالية ، لها عنصر الوحدة ، $\mathbb{C}$ حقل فإنه ينتج من النظرية (١-٣-١١) أن $[X^2+1]$ مثالى أعظم فى $\mathbb{R}[X]$

<u>مثال ٦</u> : برهن على أن : المثالى $[X^2+\bar{1}]$ ليس مثالياً أولياً فى الحلقة $\mathbb{Z}/2\mathbb{Z}[X]$ (حلقة كثيرات الحدود التى معاملاتها $\bar{0}$ ، $\bar{1}$)

<u>البرهان</u> :

$$(X+\bar{1})^2=X^2+\bar{2}X+\bar{1}=X^2+\bar{1}\in[X^2+\bar{1}]\in(\mathbb{Z}/2\mathbb{Z})[X]$$

لكن $X+\bar{1}$ ليس عنصراً فى $[X^2+\bar{1}]$

<u>مثال ٧</u> : لتكن R حلقة جميع الدوال (الرواسم) المتصلة من $\mathbb{R}$ إلى $\mathbb{R}$. برهن على أن $A:=\{f\in R\mid f(0)=0\}$ مثالى أعظم فى R .

<u>البرهان</u> : نبرهن أولاً على أن A مثالى فى R .

$\hat{0}\in A$ (الراسم الصفرى) لأن $\hat{0}(0)=0$ أى أن $A\neq\phi$

$$f-g\in A \quad \Leftarrow (f-g)(0)=f(0)-g(0)=0 \Leftarrow f,g\in A$$

$$\left.\begin{array}{l} gf\in A \quad \Leftarrow (gf)(0)=g(0)f(0)=g(0)0=0, \\ fg\in A \quad \Leftarrow (fg)(0)=f(0)g(0)=0g(0)=0 \end{array}\right\} \quad g\in R \text{ ، } f\in A$$

أى أن A مثالى فى R . والآن نعرف الراسم

$$\varphi: R\to\mathbb{R}$$
$$f\mapsto f(0)$$

φ هومومورفيزم، φ شامل (غامر ، فوقى)، $Ker(\varphi)=A$، ثم طبق النظرية (١-٣-٣) . ومن حيث إن $\mathbb{R}$ حقل ، R إبدالية ، ذات عنصر وحدة ، ينتج المطلوب من النظرية (١-٣-١١) ، كما سبق فى مثال٥ السابق .

مثال٨ : اعتبر $\mathbb{Z}/_{5\mathbb{Z}}[X]$ (حلقة كثيرات الحدود فى X التى معاملاتها $\bar{0}$ ، $\bar{1}$ ، ... ، $\bar{4}$).

أوجد المعكوس الضربى لــ $\bar{2}X+\bar{3}+I$ حيث $I=[X^2+X+\bar{2}]$ فى الحلقة $(\mathbb{Z}/_{5\mathbb{Z}})[X]/_I$

الحل : ليكن المعكوس الضربى للعنصر $\bar{2}X+\bar{3}+I$ هو $aX+b+I$ حيث $a,b\in\{\bar{0},...,\bar{4}\}$. والآن لدينا

$$(\bar{2}X+\bar{3}+I)(aX+b+I)=\bar{1}+I$$

أى أن

$$\bar{2}aX^2+(\bar{3}a+\bar{2}b)X+\bar{3}b-\bar{1}\in I$$

$$\Rightarrow \bar{2}aX^2+(\bar{3}a+\bar{2}b)X+\bar{3}b-1=\lambda(X^2+X+\bar{2})$$

$$\Rightarrow \bar{2}a=\lambda \qquad (1),$$
$$\bar{3}a+\bar{2}b=\lambda \qquad (2),$$
$$\bar{3}b-\bar{1}=\bar{2}\lambda \qquad (3)$$

من (1) ، (2) ينتج أن $\bar{5}a+\bar{2}b=\bar{2}\lambda$ أى أن (4) $\bar{2}b=\bar{2}\lambda$. ومن (3) ، (4) ينتج أن $\bar{3}b-\bar{1}=\bar{2}b$ أى أن $b=\bar{1}$. ومن (4) ينتج أن $\lambda=\bar{1}$. ومن (1) ينتج أن $a=\bar{3}$. أى أن المعكوس هو $\bar{3}x+\bar{1}+I$

مثال ٩ : اوجد جميع عناصر $\mathbb{Z}[i]/[3+i]$

الحل : لاحظ أن $(3-i)(3+i)=10$. وبالتالى فإن $10+[3+i]=0+[3+i]$ (لأن $(3+i)(3-i)\in[3+i]$) وكذلك فإن $i+[3+i]=-3+[3+i]=7+[3+i]$

ومن ثم فإن $\mathbb{Z}[i]/[3+i]=\{0+[3+i],1+[3+i],...,9+[3+i]\}$

مثال ١٠ : برهن على أن $(\mathbb{Z}/3\mathbb{Z})[X]/[X^2+X+1]$ ليس نطاقاً متكاملاً .

($(\mathbb{Z}/3\mathbb{Z})[X]$ حلقة كثيرات الحدود ذات المعاملات $\bar{0}$ ، $\bar{1}$ ، $\bar{2}$)

البرهان : $X^2+X+\bar{1}=X^2-\bar{2}X+\bar{1}=(X-\bar{1})^2\in[X^2+X+\bar{1}]$

ولكن $X-\bar{1}\notin[X^2+X+\bar{1}]$ وبالتالى فإن $[X^2+X+\bar{1}]$ ليس مثالياً أولياً فى $(\mathbb{Z}/3\mathbb{Z})[X]$ ، وبالتالى فإن $(\mathbb{Z}/3\mathbb{Z})[X]/[X^2+X+\bar{1}]$ ليس نطاقاً متكاملاً (١-٣-٩) .

مثال ١١ : برهن على أن $[X^2+X+\bar{1}]$ مثالى أعظم فى الحلقة $(\mathbb{Z}/2\mathbb{Z})[X]$

البرهان : سنبرهن على أن $(\mathbb{Z}/2\mathbb{Z})[X]/[X^2+X+1]$ حقل ، وبالتالى ينتج المطلوب مباشرة (١-٣-١١) .

$(\mathbb{Z}/2\mathbb{Z})[X]$ حلقة إبدالية لها عنصر الوحدة $\bar{1}$ يختلف عن $\bar{0}$ (صفرها) وبالتالى فإن $(\mathbb{Z}/2\mathbb{Z})[X]/[X^2+X+\bar{1}]$ حلقة إبدالية عنصر الوحدة فيها هو $\bar{1}+[X^2+X+\bar{1}]$

وعنصرها الصفرى هو $[X^2+X+\bar{1}]$. وهى تتكون بالضبط من أربعة عناصر: عنصرها الصفرى ، عنصر الوحدة ،

$X+[X^2+X+\bar{1}]$ ، $\bar{1}+X+[X^2+X+\bar{1}]$. لاحظ أن

$$X^2+[X^2+X+\bar{1}]=-\bar{1}-X+[X^2+X+\bar{1}]=\bar{1}+X+[X^2+X+\bar{1}],$$

$$\bar{1}+X^2+[X^2+X+\bar{1}]=-X+[X^2+X+\bar{1}]=X+[X^2+X+\bar{1}],$$

$$X+X^2=-\bar{1}+[X^2+X+\bar{1}]=\bar{1}+[X^2+X+\bar{1}]$$

$$\bar{1}+X+X^2+[X^2+X+\bar{1}]=[X^2+X+\bar{1}],$$

والمعكوس الضربى لـ $X+[X^2+X+\bar{1}]$ هو $\bar{1}+X+[X^2+X+\bar{1}]$ لأن

$$(X+[X^2+X+\bar{1}])(\bar{1}+X+[X^2+X+\bar{1}])=X+X^2+[X^2+X+\bar{1}]$$

عنصر الوحدة فى الحلقة $=\bar{1}+[X^2+X+\bar{1}]$

أى أن $\dfrac{(\mathbb{Z}/2\mathbb{Z})[X]}{[X^2+X+\bar{1}]}$ حقل . نهاية البرهان .

<u>مثال ١٢</u> : لتكن R حلقة جميع الدوال المتصلة من $\mathbb{R}$ إلى $\mathbb{R}$. ولتكن $A:=\{f\in R\,|\,f(0)=2n, n\in\mathbb{Z}\}$. برهن على أن A حلقة جزئية من R ، لكنه ليس مثالياً فى R .

<u>البرهان</u> : $\hat{0}\in A$ (الراسم الصفرى) ، أى أن $A\neq\phi$. (الراسم الصفرى دالة متصلة)

ليكن $f,g\in A$ ينتج أن : $(n,k\in\mathbb{Z})$ $\quad (f-g)(0)=f(0)-g(0)=2n-2k$

$$=2(n-k)\in 2\mathbb{Z}$$

(بدهى أن $f-g$ دالة متصلة)

$$(fg)(0)=f(0)g(0)=2n.2k-2.2nk\in\mathbb{Z}$$

أى أن A حلقة جزئية من R . (fg دالة متصلة)

والآن لتكن $f=2$ ، $g=\sqrt{3}$ دالتين متصلتين ، $f\in A$ ، $g\in R$. لكن $(fg)(0)=2\sqrt{3}\notin A$. أى أن A ليس مثالياً فى R .

مثال١٣ : بالرجوع إلى مثال ١١ فى (١-٣-٦) برهن على أن :

(أ) $N \subset \sqrt{N}$

(ب) $\sqrt{\sqrt{N}} = \sqrt{N}$

(جـ) إذا كان N مثالياً أولياً فإن $\sqrt{N} = N$

البرهان : (أ) لبعض $n \in \mathbb{N}$ $\quad x^n \in N \quad \Rightarrow \quad x \in N$

N مثالى

$$\Rightarrow x \in \sqrt{N} \qquad \Rightarrow \quad N \subset \sqrt{N}$$

(ب) من (أ) لدينا : $\sqrt{N} \subset \sqrt{\sqrt{N}}$. والآن :

$$x \in \sqrt{\sqrt{N}} \Rightarrow \exists n \in \mathbb{N} : x^n \in \sqrt{N} \Rightarrow \exists m, n \in \mathbb{N} : x^{mn} = (x^n)^m \in N$$

$$\underset{mn \in \mathbf{N}}{\Rightarrow} x \in \sqrt{N} \Rightarrow \sqrt{\sqrt{N}} \subset \sqrt{N}$$

$$\Rightarrow \sqrt{\sqrt{N}} = \sqrt{N}$$

(جـ) من (أ) لدينا : $N \subset \sqrt{N}$. والآن :

$$x \in \sqrt{N} \Rightarrow \exists n \in \mathbb{N} : x^n \in N \Rightarrow \exists n \in \mathbb{N} : x \in N \quad \text{أو} \quad x^{n-1} \in N$$

$$\Rightarrow ... \Rightarrow x \in N \Rightarrow \sqrt{N} \subset N \Rightarrow \sqrt{N} = N.$$

مثال ١٤ : لتكن $R = \mathbb{Z}/27\mathbb{Z}$. اوجد :

(أ) $\sqrt{[\overline{0}]}$ (ب) $\sqrt{[\overline{3}]}$ (جـ) $\sqrt{[\overline{9}]}$

الحل : من مثال ١١ : $\sqrt{N} := \{a \in R \mid a^n \in N \quad , \quad n \in \mathbb{N}$ لبعض $\}$

$$\sqrt{[\overline{0}]} := \{\overline{a} \in \mathbb{Z}/27\mathbb{Z} \mid \overline{a}^n \in [\overline{0}] \quad , \quad n \in \mathbb{N} \text{ لبعض } \}$$

$$= \{\overline{a} \in \mathbb{Z}/27\mathbb{Z} \mid \overline{a}^n \in [0] + 27\mathbb{Z} \quad , \quad n \in \mathbb{N} \text{ لبعض } \}$$

$$= \{\overline{a} \in \mathbb{Z}/27\mathbb{Z} \mid a^n \in 27\mathbb{Z} \quad , \quad n \in \mathbb{N} \text{ لبعض } \}$$

$$= \{\bar{a} \in \mathbb{Z}/_{27\mathbb{Z}} \mid a = 0, \pm 3, \pm 6, \pm 9, \ldots, \pm 24, \pm 27, \ldots\} \qquad (\bar{0} = \overline{27})$$

$$= [\bar{3}]$$

(لاحظ أن $([\bar{a}] = \overline{[a]})$

ب) $\sqrt{[\bar{3}]} = \{\bar{a} \in \mathbb{Z}/_{27\mathbb{Z}} \mid \bar{a}^n \in [3] + 27\mathbb{Z} \quad , \quad n \in \mathbb{N}$ لبعض $\}$

$= \{\bar{a} \in \mathbb{Z}/_{27\mathbb{Z}} \mid a^n - 3m \in 27\mathbb{Z} \ , \ m \in \mathbb{Z}$ ولبعض $n \in \mathbb{N}$ لبعض $\}$

$$= \{\bar{a} \in \mathbb{Z}/_{27\mathbb{Z}} \mid a = 0, \pm 3, \pm 6, \ldots\}$$

$$= [\bar{3}]$$

جـ) $\sqrt{[\bar{9}]} = \{\bar{a} \in \mathbb{Z}/_{27\mathbb{Z}} \mid \bar{a}^n \in [9] + 27\mathbb{Z} \ , \ n \in \mathbb{N}$ لبعض $\}$

$= \{\bar{a} \in \mathbb{Z}/_{27\mathbb{Z}} \mid a^n - 9m \in 27\mathbb{Z} \ , \ m \in \mathbb{Z}$ ولبعض $n \in \mathbb{N}$ لبعض $\}$

$$= \{\bar{a} \in \mathbb{Z}/_{27\mathbb{Z}} \mid a = 0, \pm 3, \pm 6, \ldots\}$$

$$= [\bar{3}]$$

مثال ١٥ : لتكن R حلقة إبدالية . برهن على أن $R/\sqrt{[0]}$ ليس بها عناصر منعدمة القوة (nilpotent) غير الصفر . (انظر مثال ١٢ فى (١-١-١٥))

البرهان : ليكن $(x+\sqrt{[0]})^n = 0+\sqrt{[0]}$ لبعض $n \in \mathbb{N}$ ، أى أن $x+\sqrt{[0]}$ منعدم القوة (وهو عنصر فى $R/\sqrt{[0]}$) . هذا يقتضى أن $x^n+\sqrt{[0]} = 0+\sqrt{[0]}$ وهذا يستلزم أن $x^n \in \sqrt{[0]}$. وبالتالى فإنه يوجد $m \in \mathbb{N}$ بحيث إن $(x^n)^m \in [0]$ أى أنه يوجد $k(=mn) \in \mathbb{N}$ بحيث إن $x^k \in [0]$ وبالتالى فإن $x \in \sqrt{[0]}$ أى أن العنصر الوحيد منعدم القوة فى $R/\sqrt{[0]}$ هو $0+\sqrt{[0]}$.

مثال ١٦ : برهن على أنه فى $C(\mathbb{R})$ (حلقة الدوال المتصلة على $\mathbb{R}$) :

$$\forall x \in \mathbb{R} \quad . \quad m_x := \{f \in C(\mathbb{R}) \mid f(x) = 0\}$$

مثالى أعظم .

البرهان : $\hat{0}$ الدالة الثابتة المعرفة كالآتى $\begin{matrix}\hat{0}:\mathbb{R}\to\mathbb{R}\\ x\mapsto 0\end{matrix}$ متصلة وتحقق الشرط $\hat{0}(x) = 0$ ، فهى عنصر فى m_x ، أى أن $m_x \neq \phi$. وإذا كان $f, g \in m_x$ فواضح أن $f - g \in m_x$.
كذلك إذا كان $f \in m_x$ ، $g \in C(\mathbb{R})$ فإن :

$$(gf)(x) = g(x)f(x) = g(x)0 = 0$$

أى أن : $gf \in m_x$ ، وكذلك $fg \in m_x$. وبالتالى فإن m_x مثالى فى $C(\mathbb{R})$.

والآن نعرف الراسم : $\begin{matrix}\varphi : C(\mathbb{R}) \to \mathbb{R}\\ f \mapsto f(x)\end{matrix}$

φ راسم غامر (شامل ، فوقى) : واضح لأنه بأخذ قيمة $r \in \mathbb{R}$ نأخذ الدالة الثابتة $f = r \in C(\mathbb{R})$ (وهى متصلة بالطبع) فيكون $\varphi(r) \doteq r$. كذلك φ هومومورفيزم :

$$\forall f, g \in C(\mathbb{R}) : \varphi(f+g) = (f+g)(x) = f(x) + g(x) = \varphi(f) + \varphi(g),$$
$$\varphi(fg) = (fg)(x) = f(x)g(x) = \varphi(f)\varphi(g)$$

والآن نحسب نواة (φ) :

$$\begin{aligned} Ker(\varphi) &= \{f \in C(\mathbb{R}) : \varphi(f) = 0\} \\ &= \{f \in C(\mathbb{R}) : f(x) = 0\} \\ &= m_x \end{aligned}$$

وبتطبيق نظرية الهومومورفيزم (١-٣-٣) نحصل على :

$$C(\mathbb{R})/m_x = C(\mathbb{R})/Ker(\varphi) = \varphi(C(\mathbb{R}) \underset{\varphi \text{ غامر}}{=} \mathbb{R}$$

ولأن $\mathbb{R}$ حقل ، $C(\mathbb{R})$ حلقة إبدالية ذات عنصر الوحدة "1" فينتج من (١-٣-١١) أن m_x مثالى أعظم فى $C(\mathbb{R})$.

مثال ١٧ : هل الراسم $\varphi:\mathbb{Z}/6\mathbb{Z}\to\mathbb{Z}/30\mathbb{Z}$, $\bar{x}\mapsto\overline{6x}$ هومومورفيزم حلقى ؟

الحل : لدينا

$$\forall x\in\mathbb{Z}:\varphi(x+6\mathbb{Z})=6x+30\mathbb{Z}$$

والآن

$$\forall x,y\in\mathbb{Z}:\varphi(x+6\mathbb{Z}+y+6\mathbb{Z})=\varphi(x+y+6\mathbb{Z})$$
$$=6(x+y)+30\mathbb{Z}=6x+6y+30\mathbb{Z}$$
$$=6x+30\mathbb{Z}+6y+30\mathbb{Z}=\varphi(x+6\mathbb{Z})+\varphi(y+6\mathbb{Z})$$
$$\varphi((x+6\mathbb{Z})(y+6\mathbb{Z}))=\varphi(xy+6\mathbb{Z})=6xy+30\mathbb{Z}$$
$$=36xy+30\mathbb{Z}=(6x+30\mathbb{Z})(6y+30\mathbb{Z})=\varphi(x)\varphi(y)$$

بعض المراجع تعتبر أن φ هومومورفيزم ، وهذا هو الذى سرنا عليه من قبل . مراجع أخرى تنص على أنه إذا كان $\varphi:R\to S$ حيث R ، S حلقتان ، لهما عنصرا وحدة 1_R ، 1_S فحتى يكون φ هومومورفيزماً يجب أن يحقق شرطاً إضافياً وهو $\varphi(1_R)=1_S$.

وإذا اعتمدنا هذا التعريف ففى حالة مثالنا الراهن $\varphi(\bar{1})=\bar{6}$

$\bar{6}$ ليس هو عنصر الوحدة فى $\mathbb{Z}/30\mathbb{Z}$ بل عنصر الوحدة فى $\mathbb{Z}/30\mathbb{Z}$ هو كذلك $\bar{1}$ أى $1+30\mathbb{Z}$ ، فلا يكون φ هومومورفيزماً .

ملحوظة : تركنا للقارئ التحقق من أن φ معرف جيداً !

مثال ١٨ : اختبر إذا ما كان الراسم : $\varphi:\mathbb{Z}/4\mathbb{Z}\to\mathbb{Z}/10\mathbb{Z}$, $x+4\mathbb{Z}\mapsto 5x+10\mathbb{Z}$ هومومورفيزماً .

الحل: نبرهن أولاً على أن φ معرف جيداً كالآتى :

ليكن $x+4\mathbb{Z}=y+4\mathbb{Z}$ حيث $x,y\in\mathbb{Z}$. ينتج أن : يوجد $k\in\mathbb{Z}$ بحيث إن $x=y+4k$ وهذا يقتضى أن :

$$\varphi(x+4\mathbb{Z}) = 5x+10\mathbb{Z} = 5(y+4k)+10\mathbb{Z}, k\in\mathbb{Z}$$
$$= 5y+20k+10\mathbb{Z}, k\in\mathbb{Z}$$
$$= 5y+10\mathbb{Z} = \varphi(y+4\mathbb{Z})$$

أى أن φ معرف جيداً .

والآن لجميع $x, y\in\mathbb{Z}$:

$$\varphi(x+4\mathbb{Z}+y+4\mathbb{Z}) = \varphi(x+y+4\mathbb{Z}) = 5(x+y)+10\mathbb{Z}$$
$$= 5x+5y+10\mathbb{Z} = 5x+10\mathbb{Z}+5y+10\mathbb{Z} = \varphi(x+4\mathbb{Z})+\varphi(y+4\mathbb{Z})$$
$$\varphi((x+4\mathbb{Z})(y+4\mathbb{Z})) = \varphi(xy+4\mathbb{Z}) = 5xy+10\mathbb{Z} = 25xy+10\mathbb{Z}$$
$$= (5x+10\mathbb{Z})(5y+10\mathbb{Z}) = \varphi(x+4\mathbb{Z})\varphi(y+4\mathbb{Z})$$

(لاحظ أن $(25+10\mathbb{Z} = 5+10\mathbb{Z})$

لكننا نلاحظ أن $\varphi(1+4\mathbb{Z}) = 5+10\mathbb{Z}$ ، عنصر الوحدة فى $\mathbb{Z}/10\mathbb{Z}$ هو $1+10\mathbb{Z}$.

المسألة الآن تتوقف على التعريف هل يكون شرطاً ضرورياً أن يتحقق: صورة عنصر الوحدة فى الحلقة R هى عنصر الوحدة فى الحلقة S حتى يكون $\varphi: R\to S$ هومومورفيزماً أم لا . ونحن لم نشترط هذا الشرط. كما ذكرنا فى المثال السابق مباشرة .

<u>مثال ١٩</u> : المطلوب تعيين جميع هومومورفيزمات الحلق من $\mathbb{Z}/12\mathbb{Z}$ إلى $\mathbb{Z}/30\mathbb{Z}$

<u>الحل</u> : سنوجد أولاً جميع هومومورفيزمات الزمر من $\mathbb{Z}/12\mathbb{Z}$ إلى $\mathbb{Z}/30\mathbb{Z}$.

نحن نعلم أن الهومومورفيزم سيتحدد تماماً إذا عرفنا صورة $\overline{1}$ (مولد الزمرة $\mathbb{Z}/12\mathbb{Z}$).

فإذا كان الهومومورفيزم هو φ ، وكان $\varphi(\overline{1}) = \overline{a}$ فإن $\varphi(\overline{x}) = \overline{ax}$ ومن نظرية لاجرانج (نظرية الزمر – (١-١٠-٣)) $Ord(\varphi(\overline{1})) = Ord(\overline{a})$ يقسم $Ord(\mathbb{Z}/30\mathbb{Z})$ أى يقسم 30 . ومن مثال٥٩ من أمثلة متنوعة فى الباب الأول من نظرية الزمر $Ord(\varphi(\overline{1})) = Ord(\overline{a})$ يقسم $Ord(\overline{1})$ أى يقسم 12. أى أن $Ord(\varphi(\overline{1})) = Ord(\overline{a})$

يقسم 12 ، 30 وبالتالى يكون $Ord(\bar{a}) \in \{1,2,3,6\}$ ، وبالتالى يكون $\bar{a}$ هو : $\bar{0}$ أو $\overline{15}$ أو $\overline{10}$ أو $\overline{20}$ أو $\bar{5}$ أو $\overline{25}$. ونترك للقارئ التحقق من أنها جميعاً تعطى هومومورفيزمات زمر.

والآن نختبر أياً من هذه هومومورفيزمات الزمر سيكون هومومورفيزم حلق : فنلاحظ أنه فى $\mathbb{Z}/12\mathbb{Z}$ يكون $\bar{1}.\bar{1} = \bar{1}$ وبالتالى فإن :

$$\bar{a} = \varphi(\bar{1}) = \varphi(\bar{1}.\bar{1}) = \varphi(\bar{1}).\varphi(\bar{1}) = \bar{a}.\bar{a}$$

فى $\mathbb{Z}/30\mathbb{Z}$ لكن $\overline{25} = \bar{5}.\bar{5} \neq \bar{5}$ فى $\mathbb{Z}/30\mathbb{Z}$ أى أن $\bar{a} = \bar{5}$ لايصلح .

كذلك فإن : $\overline{10} = \overline{400} = \overline{20}.\overline{20} \neq \overline{20}$ أى أن $\bar{a} = \overline{20}$ كذلك لايصلح .

$\bar{a} = \bar{0}, \overline{15}, \overline{10}, \overline{25}$ جميعاً تحقق $\bar{a} = \bar{a}.\bar{a}$ ، ويترك للقارئ التحقق من أنها جميعاً تعرف هومومورفيزمات حلق .

<u>مثال ٢٠</u> : اعتبر المتوالية 3 ، 7 ، 11 ، 15 ، ... هل من الممكن أن يكون أحد حدود هذه المتوالية يساوى مجموع مربعين لعددين صحيحين ؟

<u>الحل</u> : الحد العام فى هذه المتوالية هو $3 + 4n$ حيث $n \in \mathbb{N}$ أى عدد طبيعى أكبر من أو يساوى الصفر. فإذا كان أحد الحدود مجموع مربعين لعددين صحيحين x،y مثلاً فإن :

$$3 + 4n = x^2 + y^2, x, y \in \mathbb{Z}$$

وبالحساب فى $\mathbb{Z}/4\mathbb{Z}$ يكون

$$\bar{3} = \bar{x}^2 + \bar{y}^2, \bar{x}, \bar{y} \in \mathbb{Z}/4\mathbb{Z}$$

وبالحساب المباشر نجد أنه لايوجد $\bar{x}, \bar{y} \in \mathbb{Z}/4\mathbb{Z}$ اللتان تحققان المعادلة . إذن لايمكن أن يكون أحد حدود المتوالية يساوى مجموع مربعى عددين صحيحين .

<u>مثال ٢١</u> : برهن على أن المتوالية 2 ، 10 ، 18 ، 26 ، ... لاتحتوى على أى مكعب

البرهان : الحد العام فى المتوالية هو $2+8k, k\in\mathbb{N}$ (k عدد طبيعى أكبر من أو يساوى الصفر). بالحساب فى $\mathbb{Z}/8\mathbb{Z}$ ، أى بالحساب مقياس 8 ، إذا كان هناك حد فى المتوالية مكعب :

$$x^3 \equiv 2 (\bmod 8) \qquad (1)$$

واضح أن x لايمكن أن تكون فردية أى أن x لاتساوى 1 أو 3 أو 5 أو 7 . وبتجربة $x=2$ ، $x=4$ ، $x=6$ يتضح أن أياً منها لايحقق (1) .

وهو المطلوب .

مثال ٢٢ : فى $\mathbb{Z}$: ليكن $A=[2]$ (المثالى المتولد من 2) ، $B=[8]$. برهن على أن الزمرة A/B تكون متشاكلة (أيزومورفية) مع $\mathbb{Z}/4\mathbb{Z}$ ، لكن الحلقة A/B لاتكون أيزومورفية مع $\mathbb{Z}/4\mathbb{Z}$

البرهان : الزمرة $2\mathbb{Z}/8\mathbb{Z}$ هى $\{8\mathbb{Z}, 2+8\mathbb{Z}, 4+8\mathbb{Z}, 6+8\mathbb{Z}\}$ ، وهى دائرية ومولدها $2+8\mathbb{Z}$ (كذلك يصلح $6+8\mathbb{Z}$ مولداً لها) وبالتالى فهى تتشاكل مع الزمرة $\mathbb{Z}/4\mathbb{Z}$ (انظر نظرية تفصيل الزمر الدائرية (١-١١-٨) فى نظرية الزمر).

الحلقة $2\mathbb{Z}/8\mathbb{Z}$ تتكون بالطبع كما سبق ، لكن ليس بها عنصر وحدة ، بينما الحلقة $\mathbb{Z}/4\mathbb{Z}$ لها عنصر الوحدة $1+4\mathbb{Z}$. وبالتالى فإن $2\mathbb{Z}/8\mathbb{Z}$ ، $\mathbb{Z}/4\mathbb{Z}$ كحلقتين تكونان غير متشاكلتين .

مثال ٢٣ : برهن على أن مجموع مربعات ثلاثة أعداد صحيحة متتالية لايمكن أن يساوى مربعاً .

البرهان : لنفترض أن الأعداد الثلاثة المتتالية هى : $x-1$ ، x ، $x+1$ حيث $x\in\mathbb{Z}$.
إذا كان الادعاء صحيحاً فإنه يوجد $y\in\mathbb{N}$ بحيث يكون :

$$(x-1)^2 + x^2 + (x+1)^2 = y^2$$
$$\Rightarrow 3x^2 + 2 = y^2$$

وبالحساب مقياس 3 نحصل على : $y^2 \equiv 2(\text{mod}\,3)$. وواضح أنه لايوجد حل لهذه المعادلة ويكون الادعاء خاطئاً .

مثال ٢٤ : قابلية القسمة على 9 :

برهن على أن العدد n ذا التمثيل العشرى $a_k a_{k-1} \dots a_1 a_0$ يكون قابلاً للقسمة على 9 إذا كان وفقط إذا كان $a_k + a_{k-1} + \dots + a_1 + a_0$ قابلاً للقسمة على 9 .

البرهان :

$$n = a_0 + 10a_1 + \dots + 10^{k-1} a_{k-1} + 10^k a_k$$

$$= a_0 + 10a_1 + \dots + \underbrace{10\dots10}_{k-1 \text{ من المرات}} a_{k-1} + \underbrace{10\dots10}_{k \text{ من المرات}} a_k$$

بالحساب فى مقياس 9 نحصل على :

$$n \equiv a_0 + a_1 + \dots + \underbrace{1\dots1}_{k-1 \text{ من المرات}} a_{k-1} + \underbrace{1\dots1}_{K \text{ من المرات}} a_k \ (\text{mod}\,9)$$

$$\Rightarrow \qquad 9 \text{ يقسم } [n - (a_0 + a_1 + \dots + a_{k-1} + a_k)]$$

أى أن n يقبل القسمة على 9 إذا كان وفقط إذا كان $a_0 + a_1 + \dots + a_{k-1} + a_k$ يقبل القسمة على 9 .

ملحوظة : لاحظ أننا عند الحساب فى المقياس 9 (وكذلك عند الحساب فى أى مقياس) استخدمنا :

$$\forall x, y \in \mathbb{Z}: \qquad \overline{x+y} = \bar{x} + \bar{y} \qquad \overline{xy} = \bar{x}.\bar{y}$$

وهذا متفق تماماً مع تعريف عمليتى الجمع والضرب فى $\mathbb{Z}/m\mathbb{Z}$ حيث $m \in \mathbb{N}$ ، حيث يعرف الجمع والضرب كالآتى :

$$\forall x, y \in \mathbb{Z}: \quad (x + m\mathbb{Z}) + (y + m\mathbb{Z}) := x + y + m\mathbb{Z},$$
$$(x + m\mathbb{Z}) + (y + m\mathbb{Z}) := xy + m\mathbb{Z}$$

أى أن $\bar{x}+\bar{y} := \overline{x+y}$ ،

$$\bar{x}.\bar{y} := \overline{xy}$$

<u>مثال ٢٥</u> : قابلية القسمة على 11 :

برهن على أن العدد n ذا التمثيل العشرى $a_k a_{k-1}...a_1 a_0$ يكون قابلا للقسمة على 11 إذا كان وفقط إذا كان $a_0 - a_1 + a_2 - ... + (-1)^k a_k$ يقبل القسمة على 11 .

البرهان : كما جاء فى مثال ٢٤ السابق مباشرة

$$n = a_0 + 10a_1 + 10^2 a_2 + ... + 10^k a_k$$

$$= a_0 + 10a_1 + (10)(10)a_2 + ... + \underbrace{10...10}_{\text{من المرات } k} a_k$$

بالحساب فى مقياس 11 نحصل على :

$$n \equiv a_0 + (-1)a_1 + (-1)^2 a_2 + ... + (-1)^k a_k (\text{mod} 11)$$

$$= a_0 - a_1 + a_2 + ... + (-1)^k a_k (\text{mod} 11)$$

أى أن 11 يقسم $[n - (a_0 - a_1 + a_2 + ... + (-1)^k a_k)]$

أى أن n يقبل القسمة على 11 إذا كان وفقط إذا كان

$a_0 - a_1 + a_2 + ... + (-1)^k a_k$ يقبل القسمة على 11 .

<u>مثال ٢٦</u> : قابلية القسمة على 4 :

ليكن n عدداً صحيحاً له التمثيل العشرى : $n = a_k a_{k-1}...a_1 a_0$

برهن على أن n يقبل القسمة على 4 إذا كان وفقط إذا كان $a_1 a_0$ يقبل القسمة على 4

<u>البرهان</u> : يمكن التعبير عن n بالكيفية الآتية :

$$n = a_1 a_0 + 10^2 a_2 + 10^3 a_3 + ... + 10^k a_k$$

ويلاحظ أن 10^m يقبل القسمة على 4 لجميع $m \geq 2$. وبالتالى فإننا بالحساب مقياس 4 نحصل على:

$$n \equiv a_1 a_0 (\text{mod} 4)$$

أى أن 4 يقسم $(n-a_1a_0)$ ، بعبارة أخرى n يقبل القسمة على 4 إذا كان وفقط إذا كان $a_1\,a_0$ يقبل القسمة على 4.

<u>مثال ٢٧</u> : ليكن m عدداً صحيحاً موجباً ، وليكن n عدداً صحيحاً موجباً ينتج من m بإعادة ترتيب "مكونات" m ، فمثلاً الرقم 72345 يعاد ترتيبه ليصبح 27453 . برهن على أن $m-n$ يقبل القسمة على 9 .

<u>البرهان</u> : ليكن العدد m هو $a_ka_{k-1}...a_1a_0$. من مثال ٢٤ m يقبل القسمة على 9 إذا كان وفقط إذا كان $a_0+a_1+...+a_{k-1}+a_k$ يقبل القسمة على 9 . ولكن إعادة ترتيب العدد m بأى شكل لايغير المجموع $S=a_0+a_1+...+a_{k-1}+a_k$ ، ويكون مجموع "مكونات" العدد n هو $b_0+b_1+...+b_{k-1}+b_k=S$ وبالتالى فإن مجموع "مكونات" العدد $m-n$ سيكون مساوياً للصفر، وهو يقبل القسمة على 9 . وبالتالى فإن العدد $m-n$ يقبل القسمة على9 .

<u>مثال ٢٨</u> : برهن على أنه فى أية حلقة إبدالية ذات عنصر الوحدة يكون كل مثالى أعظم فيها مثالياً أولياً

<u>البرهان</u> : لتكن R حلقة إبدالية ذات عنصر الوحدة ، ليكن $m\subset R$ مثالياً أعظم . هذا يستلزم أن R/m حقل (١-٣-١١) $\Leftarrow$ R/m نطاق متكامل $\Leftarrow$ m مثالى أولى فى R (١-٣-٩)

<u>مثال ٢٩</u> : لتكن R حلقة إبدالية . وليكن A ، B مثاليين أعظمين ، $A\neq B$. عندئذ فإن A ، B متعاظمان معاً. (انظر مثال١ فى (١-٢-٩))

<u>البرهان</u> : ليكن $A+B\neq R$ ، هذا يقتضى أن $A+B=A$ (لأن A مثالى أعظم) وهذا يقتضى أن $B\subset A$. ولكن B مثالى أعظم ، $A\neq R$ فينتج أن $B=A$: تناقض .

(تذكر أن مجموع مثاليين = مثالياً) .

<u>مثال ٣٠</u>: لتكن $A,B_1,B_2,...,B_n\subset R$ مثاليات فى حلقة إبدالية R . برهن على أنه إذا كان لكل i ،

$1\leq i\leq n$: A,B_i متعاظمان معا ، فإن $A,B_1B_2...B_n$ متعاظمان معا .

البرهان : سنبرهن أولاً على أن : A ، B متعاظمان معاً $\Leftrightarrow$ $\rho(B)=R/A$ حيث

$\rho: R \to R/A$ الإبيمورفيزم الطبيعي

A ، B متعاظمان معاً $\Leftrightarrow \rho(B)=B/A=(B+A)/A=R/A$

$$\left((B+A)/A=\{b+a+A \mid b\in B, a\in A\}=\{b+A \mid b\in B\}=B/A\right)$$

والآن :

$$\rho(B_1B_2...B_n) \quad = \quad \rho(B_1)\rho(B_2)...\rho(B_n)$$

ρ هومومورفيزم

$$=(R/A)(R/A)...(R/A)=R/A$$

$\Rightarrow$ $A, B_1B_2...B_n$ متعاظمان معاً

مثال ٣١ : إذا كانت A_1 ، A_2، ... مثاليات متعاظمة معا مثنى مثنى فى حلقة إبدالية R فإن

$$A_1...A_n = A_1 \cap ... \cap A_n$$

البرهان : بالاستقراء الرياضى على n

$n=2$: انظر مثال١ فى جبر المثاليات (١-٢-٩) (*)

$n \to n+1$: لتكن A_1 ، A_2 ، ... ، A_{n+1} مثاليات متعاظمة معاً مثنى مثنى ، ينتج من مثال ٣٠ السابق مباشرة أن $A_1A_2...A_n, A_{n+1}$ متعاظمان معاً . ومن ثم فإن

$$(A_1A_2...A_n)A_{n+1} \underset{(*)}{=} (A_1...A_n)\cap A_{n+1}$$

$$= \quad (A_1\cap...\cap A_n)\cap A_{n+1} = A_1\cap...\cap A_n\cap A_{n+1}$$

فرض الاستقراء

مثال ٣٢ : ليكن R ، S حلقتين إبداليتان لهما عنصرا الوحدة 1_R ، 1_S ، φ هومومورفيزم غامراً (إبيمورفيزم) من R على S ، A مثالياً فى S .

إذا كان A مثالياً أعظم فى S فبرهن على أن $\varphi^{-1}(A)$ مثالى أعظم فى R وذلك بفرض أن $\varphi^{-1}(A) \neq R$.

<u>البرهان</u> : نعتبر الهومومورفيزم

$$\rho : R \to S/A$$
$$x \mapsto \varphi(x) + A$$

$$\forall x, y \in R : \rho(x+y) = \varphi(x+y) + A = \varphi(x) + \varphi(y) + A$$
$$= \varphi(x) + A + \varphi(y) + A = \rho(x) + \rho(y)$$

$$\rho(xy) = \varphi(xy) + A = \varphi(x)\varphi(y) + A = (\varphi(x) + A)(\varphi(y) + A)$$
$$= \rho(x)\rho(y)$$

إذن ρ هومومورفيزم

كذلك ρ شامل (غامر ، فوقى) لأن φ شامل

نحسب نواة (ρ)

$$Ker(\rho) = \{x \in R \mid \varphi(x) + A = A\}$$

(تذكر أن A هو الصفر فى الحلقة S/A)

$$= \{x \in R \mid \varphi(x) \in A\} = \varphi^{-1}(A)$$

والآن نطبق نظرية الهومومورفيزم (١-٣-٣) :

$$R/\varphi^{-1}(A) = R/Ker(\rho) \cong \rho(R) = S/A$$

A مثالى أعظم فى S وإذن S/A حقل (١-٣-١١) ، أى أن $R/\varphi^{-1}(A)$ حقل ، وبالتالى فإن $\varphi^{-1}(A)$ مثالى أعظم فى R .

<u>**مثال ٣٣**</u> : ليكن n قاسماً لـــ m ، a عنصراً متماثل القوة فى $\mathbb{Z}_n$ (أى أن $a^2 = a$ كما جاء فى مثال ١٠ (١-١-١٥)) . برهن على أن الراسم $\overline{x} \mapsto \overline{ax}$ هومومورفيزم من

$\mathbb{Z}_m$ إلى $\mathbb{Z}_n$. برهن كذلك على أن نفس التناظر ليس بالضرورة راسماً معرفاً جيداً إذا لم يكن n قاسماً لـــ m .

البرهان : ليكن $kn = m$ حيث $k \in \mathbb{N}$ ، $k \neq 0$. نعتبر :

$$\varphi: \mathbb{Z}_{kn} \to \mathbb{Z}_n$$
$$x + kn\mathbb{Z} \mapsto ax + n\mathbb{Z}$$

φ معرف جيداً : ليكن

$$x + kn\mathbb{Z} = y + kn\mathbb{Z}$$
$$\Rightarrow \exists z \in \mathbb{Z} : x + knz = y$$
$$\Rightarrow \varphi(y + kn\mathbb{Z}) = ay + n\mathbb{Z} = a(x + knz) + n\mathbb{Z}$$
$$= ax + aknz + n\mathbb{Z} = ax + n\mathbb{Z} = \varphi(x + kn\mathbb{Z})$$

والآن ندرس الحالة إذا كان n ليس قاسماً لـــ m :

ليكن $a = 1$ ، $m = 4$ ، $n = 3$ ، $x = 7$ ، $y = 3$:

$$\overline{x} = 7 + 4\mathbb{Z} = 3 + 4\mathbb{Z} = \overline{y}$$
$$\Rightarrow \varphi(\overline{x}) = \varphi(7 + 4\mathbb{Z}) = 7 + 3\mathbb{Z} = 4 + 3\mathbb{Z} \neq 0 + 3\mathbb{Z}$$
$$= 3 + 3\mathbb{Z} = \varphi(3 + 4\mathbb{Z}) = \varphi(\overline{y})$$

والآن φ هومومورفيزم (إذا كان φ معرفاً جيداً) :

$$\forall \overline{x}, \overline{y} \in \mathbb{Z}_{kn} : \varphi(x + kn\mathbb{Z} + y + kn\mathbb{Z}) = \varphi(x + y + kn\mathbb{Z})$$
$$= a(x + y) + n\mathbb{Z} = ax + ay + n\mathbb{Z}$$
$$= ax + n\mathbb{Z} + ay + n\mathbb{Z} = \varphi(x + kn\mathbb{Z}) + \varphi(y + kn\mathbb{Z})$$

$$\varphi((x + kn\mathbb{Z})(y + kn\mathbb{Z})) = \varphi(xy + kn\mathbb{Z}) = axy + n\mathbb{Z} \underset{a^2 = a}{=} a^2xy + n\mathbb{Z}$$
$$= \quad axay + n\mathbb{Z} = (ax + n\mathbb{Z})(ay + n\mathbb{Z}) = \varphi(x + kn\mathbb{Z})\varphi(y + kn\mathbb{Z})$$

$\mathbb{Z}_n$ إبدالية

تمارين

(١) اكتب جدولى الجمع والضرب لـ $2\mathbb{Z}/8\mathbb{Z}$. هل الحلقتان $2\mathbb{Z}/8\mathbb{Z}$ ، $\mathbb{Z}_4$ تتشاكلان ؟

(إرشاد : $\mathbb{Z}_4$ تتشاكل مع $\mathbb{Z}/4\mathbb{Z}$ ، ولكنها لاتتشاكل مع $2\mathbb{Z}/8\mathbb{Z}$ لأن $2\mathbb{Z}/8\mathbb{Z}$ ليس لها عنصر وحدة . اكتب التفاصيل وانظر مثال٢٢ فى (١-٣-٢٠))

(٢) برهن على أن N مثالى أعظم فى حلقة R إذا كان وفقط إذا كان R/N حلقة بسيطة ، أى أن R/N لاتحتوى على مثالى فعلى .

(٣) لتكن $R=\{\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \mid a_i \in \mathbb{Z}\}$ ، وليكن I مجموعة جزئية من R يتكون من جميع المصفوفات ذات المداخل (entries) (أو العناصر) الزوجية . برهن على أن I مثالى فى R ، واوجد عدد عناصر R/I .

(٤) اوجد جميع المثاليات العظمى فى $\mathbb{Z}/36\mathbb{Z}$ ، $\mathbb{Z}/10\mathbb{Z}$ ، $\mathbb{Z}/n\mathbb{Z}$

(٥) برهن على أن المثالى $[X^2+1]$ مثالى أولى فى $\mathbb{Z}[X]$ ، لكنه ليس أعظم فى $\mathbb{Z}[X]$ (لاحظ أن المثالى نفسه أعظم فى $\mathbb{R}[X]$. مثال٥ فى (١-٣-٢٠))

(٦) أنشئ جدول الضرب للحلقة $3\mathbb{Z}/9\mathbb{Z}$

(٧) برهن على أن $\mathbb{R}[X]/[X^2+1]$ حقل

(٨) برهن على أنه فى $\mathbb{Z}[X]$ حلقة كثيرات الحدود ذات المعاملات الصحيحة يكون $I=\{f\in\mathbb{Z}[X] \mid f(0)=0\}$ ليس مثالياً أعظم .

(٩) لتكن $\mathbb{R}=\mathbb{Z}/36\mathbb{Z}$. احسب :

(أ) $\sqrt{[\bar{0}]}$ (ب) $\sqrt{[\bar{4}]}$ (جـ) $\sqrt{[\bar{6}]}$

(١٠) برهن على أن $I = [2+2i]$ ليس مثالياً أولياً فى $\mathbb{Z}[i]$. كم عدد عناصر $\mathbb{Z}[i]/I$ ؟

(١١) فى $\mathbb{Z}[X]$ ليكن $I := \{f \in \mathbb{Z}[X] \mid f(0) = 2n, n \in \mathbb{Z}\}$. برهن على أن I مثالى أولى فى $\mathbb{Z}[X]$.

(١٢) لتكن R حلقة إبدالية ، ولتكن A أية مجموعة جزئية من R . برهن على أن مبيد A (annihilator of A)

$$Ann(A) := \{r \in R \mid ra = 0 \quad \forall a \in A\}$$

يكون مثالياً فى R .

(١٣) اكتب جميع العناصر فى الحقل $\mathbb{Z}_2[X]/[X^2+X+1]$ وانشئ جدولى الجمع والضرب

(١٤) لتكن R حلقة إبدالية ، ليس لها عنصر الوحدة . صف أصغر مثالى فى R بحيث يحتوى على العنصر a .

(١٥) إذا كان R نطاق مثاليات أساسية ، وكان I مثالياً فى R فبرهن على أن كل مثالى فى R/I سيكون مثالياً أساسياً .

(١٦) برهن على أن $\mathbb{Z}[i]/[1-i]$ حقل . كم عدد عناصره ؟

(١٧) هل الراسم $\varphi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}, \; x \mapsto 6x$ هومومورفيزم حلقى ؟

(١٨) برهن على أن التناظر $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_{10}, \; x \mapsto 5x$ يحفظ عمليتى الجمع والضرب ولكنه ليس معرفاً جيداً ، وبالتالى فهو ليس راسماً وليس هومومورفيزماً .

(١٩) برهن على أن التناظر $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_{12}, \; x \mapsto 3x$ معرف جيداً ، ويحفظ عملية الجمع ، لكنه لايحفظ عملية الضرب

(٢٠) طبق نظرية الهومومورفيزم على التمرين (٢٣) من تمارين الجزء (١-٢)

(٢١) هل الراسم $\begin{matrix}\varphi:\mathbb{Z}_{10}\to\mathbb{Z}_{10}\\ x\mapsto 2x\end{matrix}$ هومومورفيزم حلق ؟

(٢٢) عين جميع الهومومورفيزمات من $\mathbb{Z}_6$ إلى $\mathbb{Z}_6$.

(٢٣) عين جميع الهومومورفيزمات من $\mathbb{Z}_{20}$ إلى $\mathbb{Z}_{30}$.

(٢٤) هل الراسم $\begin{matrix}\varphi:\mathbb{Z}_{5}\to\mathbb{Z}_{30}\\ x\mapsto 6x\end{matrix}$ هومومورفيزم حلق ؟

(٢٥) برهن على أن الرقم 7, 176, 825, 942, 116, 027, 211 يقبل القسمة على 9 ، لكنه لايقبل القسمة على 11 .

(٢٦) برهن على أن الرقم 9, 897, 654, 527, 609, 877 يقبل القسمة على 99 .

(٢٧) بدون استخدام الورقة والقلم احسب :

$(2.10^{75}+2)^{100} \pmod 3$ ، $(10^{100}+1)^{99} \pmod 3$

(٢٨) فى مثال ٢٣ من (١-٢-٨) كانت R' نطاقاً متكاملاً . اضرب مثالاً لبيان أنه إذا كانت R' ليست نطاقاً متكاملاً فإن التقرير $f(1)$ يكون عنصر الوحدة فى R' ليس صحيحاً بالضرورة .

(إرشاد : اعتبر الهومومورفيزم $\begin{matrix}\varphi:\mathbb{Z}_{5}\to\mathbb{Z}_{30}\\ x\mapsto 6x\end{matrix}$. تذكر أن $\mathbb{Z}_{30}$ ليس نطاقاً متكاملاً لأنه ليس خالياً من القواسم الصفرية)

(٢٩) برهن على أن أى هومومورفيزم من حقل <u>على</u> حلقة تتكون من أكثر من عنصر واحد يكون تشاكلاً (أى أن الإبيمورفيزم يكون أيزومورفيزماً) .

<u>**١-٣-٢١ تعريف**</u> : لتكن R_1 ، R_2 حلقتين . يعرف حاصل الضرب المباشر للحلقتين R_1 ، R_2 ، ويرمز له بالرمز $R_1\otimes R_2$ كالآتى :

$$R_1\otimes R_2 := \{(a_1,a_2)\mid a_1\in R_1, a_2\in R_2\}$$

وتعرف العمليتان "+" ، "." كما – هو متوقع – كما يلى :

$$(a_1,a_2)+(b_1,b_2) := (a_1+b_1, a_2+b_2),$$
$$(a_1,a_2).(b_1,b_2) := (a_1b_1, a_2b_2)$$

ويترك للقارئ التحقق من أن حاصل الضرب المباشر للحلقتين

R_2 ، R_1 (The direct product of the two rings) هو حلقة.

لاحظ أن العنصر الصفرى سيكون $(0,0)$ ، ومعكوس العنصر (a_1,a_2) بالنسبة لعملية الجمع هو العنصر $(-a_1,-a_2)$

١-٣-٢٢ ملحوظة : نعرف $R'_1 := \{(a_1,0) \in R_1 \otimes R_2\}$ ، $R'_2 := \{(0,a_2) \in R_1 \otimes R_2\}$

نعرف كذلك الإسقاط (projection) $\begin{matrix} p_1 : R_1 \otimes R_2 \to R'_1 \\ (a_1,a_2) \mapsto (a_1,0) \end{matrix}$. p_1 هومومورفيزم لأن :

$$\forall (a_1,a_2),(b_1,b_2) \in R_1 \otimes R_2 : p_1((a_1,a_2)+(b_1,b_2)) = p_1(a_1+b_1, a_2+b_2)$$

$$= (a_1+b_1, 0) = (a_1,0)+(b_1,0) = p_1(a_1,a_2)+p_1(b_1,b_2),$$

$$p_1((a_1,a_2).(b_1,b_2)) = p_1(a_1b_1, a_2b_2) = (a_1b_1,0) = (a_1,0).(b_1,0) = p_1(a_1,a_2).p_1(b_1,b_2)$$

p_1 راسم غامر(شامل ، فوقى) : واضح . نحسب نواة (p_1) :

$$\begin{aligned} Ker(p_1) &= \{(a_1,a_2) \in R_1 \otimes R_2 \mid p_1(a_1,a_2) = (0,0)\} \\ &= \{(a_1,a_2) \in R_1 \otimes R_2 \mid (a_1,0) = (0,0)\} \\ &= \{(0,a_2) \in R_1 \otimes R_2\} = R'_2 \end{aligned}$$

ونطبق نظرية الهومومورفيزم (١-٣-٣) فنحصل على :

$$R_1 \otimes R_2 \big/ R'_2 = R_1 \otimes R_2 \big/ Ker(p_1) \cong p_1(R_1 \otimes R_2) \underset{p_1 \text{ غامر}}{=} R'_1$$

نستنتج كذلك أن R'_2 مثالى فى $R_1 \otimes R_2$ (مثال ١٨ فى (١-٢-٨))

وبالمثل نعرف الإسقاط :

$$\begin{matrix} p_2 : R_1 \otimes R_2 \to R'_2 \\ (a_1,a_2) \mapsto (0,a_2) \end{matrix}$$

p_2 هومومورفيزم (كما سبق فى p_1) ، غامر ، $Ker(p_2) = R'_1$

وبتطبيق نظرية الهومومورفيزم (كما سبق) ينتج أن :

$$R_1 \otimes R_2 / R'_1 = R_1 \otimes R_2 / Ker(p_2) \cong p_2(R_1 \otimes R_2) = R'_2$$

p_2 غامر

كذلك فإن R'_1 مثالى فى $R_1 \otimes R_2$

نلاحظ كذلك أن $R'_1 \cong R_1$ ، $R'_2 \cong R_2$. ويمكن رؤية ذلك ببساطة كالآتى: نعرف :

$$\varphi_1 : R'_1 \to R_1$$
$$(a_1, 0) \mapsto a_1$$

φ_1 غامر (شامل) : واضح

φ_1 واحد لواحد :

$$\varphi_1(a_1,0) = \varphi_1(b_1,0) \Rightarrow a_1 = b_1 \Rightarrow (a_1,0) = (b_1,0)$$

φ_1 هومومورفيزم

$$\forall (a_1,0),(b_1,0) \in R'_1 : \varphi_1((a_1,0)+(b_1,0)) = \varphi_1(a_1+b_1,0) = a_1+b_1 = \varphi_1(a_1,0)+\varphi_1(b_1,0)$$

$$\varphi_1((a_1,0).(b_1,0)) = \varphi_1(a_1b_1,0) = a_1b_1 = \varphi_1(a_1,0).\varphi_1(b_1,0)$$

$\Rightarrow$ φ أيزومورفيزم

بالمثل نعرف $\begin{aligned}\varphi_2 &: R'_2 \to R_2 \\ (0,a_2) &\mapsto a_2\end{aligned}$ وينتج أن φ_2 أيزومورفيزم ويكون $R'_2 \cong R_2$

<u>١-٣-٢٣ ملحوظة</u> :

(أ) كل عنصر $(a_1,a_2) \in R_1 \otimes R_2$ يمكن التعبير عنه فى صورة مجموع عنصرين أحدهما فى R'_1 والآخر فى R'_2 وبطريقة وحيدة :

$$(a_1,a_2) = (a_1,0) + (0,a_2)$$

(ب) حاصل ضرب عنصرين أحدهما فى R'_1 والآخر فى R'_2 هو $(0,0) \in R_1 \otimes R_2$:

$$\forall a_1 \in R_1 \quad \forall a_2 \in R_2 : (a_1,0).(0,a_2) = (a_1 0, 0 a_2) = (0,0)$$

(جـ) بصفة عامة فإننا يمكننا أن نعبر عن حاصل الضرب المباشر للحلقات R_1 ، R_2 ، ... ، R_n ونرمز لذلك بالرمز $R_1 \otimes R_2 \otimes ... \otimes R_n$. ونعرف كذلك المثاليات R'_1 ، R'_2 ، ... ، R'_n فى حاصل الضرب $R_1 \otimes R_2 \otimes ... \otimes R_n$. ونحصل على التشاكلات (الأيزومورفيزمات): $R'_1 \cong R_1$ ، $R'_2 \cong R_2$ ، ... ، $R'_n \cong R_n$

<u>١-٣-٢٤ تعريف</u> :

يقال لحلقة R إنها حاصل الجمع المباشر لحلقتين جزئيتين

(The direct sum of two subrings)

R_1 ، R_2 إذا كان :

(١) كل عنصر فى R يعبر عنه بطريقة وحيدة كحاصل جمع عنصرين أحدهما فى R_1 والآخر فى R_2

(٢) إذا كان $x, y \in R$ بحيث إن : $x = x_1 + x_2$ ، $y = y_1 + y_2$ حيث $x_1, y_1 \in R_1$ ، $x_2, y_2 \in R_2$ فإن :

$$xy = (x_1 + x_2)(y_1 + y_2) = x_1 y_1 + x_2 y_2$$

وسنكتب للتعبير عن أن R هى حاصل الجمع المباشر للحلقتين الجزئيتين R_1 , R_2 :

$$R = R_1 \oplus R_2$$

<u>١-٣-٢٥ ملحوظة</u> :

إذا كان $R = R_1 \oplus R_2$ فإن $R/R_1 \cong R_2$ ، $R/R_2 \cong R_1$

<u>البرهان</u> : نعرف الراسم

$$\varphi : R_1 \oplus R_2 \to R_2$$
$$x_1 + x_2 \mapsto x_2$$

الراسم φ **<u>معرف جيدا</u>** لأن كل عنصر فى $R_1 \oplus R_2$ يعبر عنه **<u>بطريقة وحيدة</u>** على الشكل $x = x_1 + x_2$ ، حيث $x_1 \in R_1$ ، $x_2 \in R_2$

φ راسم غامر (شامل) : واضح

φ هومومورفيزم لأن :

$$\forall x_1 + x_2, y_1 + y_2 \in R_1 \oplus R_2 :$$

$$\varphi((x_1+x_2)+(y_1+y_2)) = \varphi(x_1+y_1+x_2+y_2) = x_2+y_2 = \varphi(x_1+x_2)+\varphi(y_1+y_2),$$

$$\varphi((x_1+x_2)(y_1+y_2)) = \varphi(x_1y_1+x_2y_2) = x_2y_2 = \varphi(x_1+x_2)\varphi(y_1+y_2)$$

وبتطبيق نظرية الهومومورفيزم (١-٣-٣) نحصل على :

$$R_1 \oplus R_2 / Ker(\varphi) \cong \varphi(R_1 \oplus R_2) = R_2$$

حيث

$$\begin{aligned} Ker(\varphi) &= \{x_1 + x_2 \mid x_1 + x_2 \in R_1 \oplus R_2, \varphi(x_1 + x_2) = x_2 = 0\} \\ &= \{x_1 + 0 \in R_1 \oplus R_2\} \\ &\cong \{x_1 \mid x_1 \in R_1\} = R_1 \end{aligned}$$

أى أن R_1 مثالى فى $R_1 \oplus R_2$ ،

$$R_1 \oplus R_2 / R_1 \cong R_2$$

وبالمثل نعرف الراسم

$$\begin{aligned} \psi : R_1 \oplus R_2 &\to R_1 \\ x_1 + x_2 &\mapsto x_1 \end{aligned}$$

ψ معرف جيداً (كما سبق φ) ، ψ غامر ، هومومورفيزم ، ونصل إلى :

$$R_1 \oplus R_2 / R_2 \cong R_1$$

حيث R_2 مثالى فى $R_1 \oplus R_2$.

<u>١-٣-٢٦ نظرية :</u>

الشروط الآتية ضرورية وكافية حتى تكون الحلقة R حاصل جمع مباشر لحلقتين جزئيتين R_1 ، R_2 فيها:

(١) R_1 ، R_2 مثاليان فى R

(٢) العنصر 0 هو العنصر الوحيد المشترك بين R_1 ، R_2

(٣) $R = R_1 + R_2$

(٤) $R_1R_2 = \{0\}$ $\quad (R_1R_2 := \{x_1x_2 \mid x_1 \in R_1, x_2 \in R_2\})$

<u>**البرهان**</u> : الشروط ضرورية : من المناقشة السابقة يتضح (١) .

إذا كان $a \in R_1 \cap R_2$ فإننا يمكننا أن نكتب $a + 0 = a = 0 + a$ ومن وحدانية التمثيل يتضح أن $a = 0$ ، ونحصل على (٢) . الشرط (٣) واضح . بالنسبة للشرط (٤) : ليكن $x_1 \in R_1$ ، $x_2 \in R_2$. لدينا :

$$x_1x_2 = (x_1 + 0)(0 + x_2) = x0 + 0x_2 = 0 + 0 = 0$$

الشروط كافية : (٣) تعنى أن كل عنصر فى R يمكن أن يكتب على صورة حاصل جمع عنصرين أحدهما فى R_1 ، والآخر فى R_2 . نحن نبرهن على أن هذا <u>**التمثيل وحيد**</u> كالآتى :

ليكن $x \in R$ ، $x = x_1 + x_2 = y_1 + y_2$ حيث $x_1, y_1 \in R_1$ ، $x_2, y_2 \in R_2$ هذا يستلزم أن : $x_1 - y_1 = y_2 - x_2$. لكن $x_1 - y_1 \in R_1$ ، $y_2 - x_2 \in R_2$ (لأن R_1 ، R_2 حلقتان جزئيتان فى R) . ولكن من (٢) العنصر 0 هو العنصر الوحيد المشترك بين R_1 ، R_2 ، وبالتالى يكون : $y_2 - x_2 = 0 = x_1 - y_1$ أى أن $x_1 = y_1$ ، $x_2 = y_2$ ، ويكون التمثيل وحيداً .

والآن ليكن $x, y \in R$ بحيث إن $x = x_1 + x_2$ ، $y = y_1 + y_2$ ، حيث $x_1, y_1 \in R_1$ ، $x_2, y_2 \in R_2$. لدينا :

$$\begin{aligned} xy = (x_1 + x_2)(y_1 + y_2) &= x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2 \\ &= x_1y_1 + 0 + 0 + x_2y_2 = x_1y_1 + x_2y_2 \end{aligned}$$

(٤)

نهاية البرهان .

<u>**١-٣-٢٧ أمثلة محلولة**</u> :

<u>**مثال ١**</u> : لتكن $R := \mathbb{Z} \otimes \mathbb{Z} \otimes \mathbb{Z}$ ، $S := \{(a,b,c) \in R \mid a + b = c\}$

برهن أو انف : S حلقة جزئية من R

الحل : $(0,1,1),(1,1,2) \in S$ بينما $(0,1,1).(1,1,2) = (0,1,2) \notin S$ وبالتالى فإن S ليس حلقة جزئية من R .

مثال ٢ : برهن أو انف : عنصر الوحدة فى حلقة جزئية يجب أن يكون هو عنصر الوحدة فى الحلقة

الحل : عنصر الوحدة فى الحلقة $\mathbb{Z} \otimes \mathbb{Z}$ هو $(1, 1)$ ، بينما عنصر الوحدة فى $\mathbb{Z} \otimes \{0\}$ ، وهى حلقة جزئية من $\mathbb{Z} \otimes \mathbb{Z}$ هو $(1, 0)$ لايساوى $(1, 1)$. إذن التقرير خاطئ .

مثال ٣ : عين الوحدات فى كل من :

(أ) $\mathbb{Z}$ (ب) $\mathbb{Z} \otimes \mathbb{Z}$

(جـ) $\mathbb{Z}_5$ (د) $\mathbb{Q}$

(هـ) $\mathbb{Z} \otimes \mathbb{Q} \otimes \mathbb{Z}$ (و) $\mathbb{Z}_4$

الحل :

(أ) $1, -1$ (ب) $(1, 1), (1, -1), (-1, 1), (-1, -1)$

(جـ) $\bar{1}, \bar{2}, \bar{3}, \bar{4}$ (د) $\forall q: \quad 0 \neq q \in \mathbb{Q}$

(هـ) $\forall q \in \mathbb{Q} \setminus \{0\} \quad (1,q,1),(1,q,-1),(-1,q,1),(-1,q,-1)$

(د) $\bar{1}, \bar{3}$

مثال ٤ : لتكن R ، S حلقتين . برهن على أن :

(أ) الراسم $\begin{array}{l} \varphi: R \otimes S \to R \\ (a,b) \mapsto a \end{array}$ هومومورفيزم حلق

(ب) الراسم $\begin{array}{l} \varphi: R \to R \otimes S \\ a \mapsto (a,0) \end{array}$ مونومورفيزم حلق

(جـ) $R \otimes S \cong S \otimes R$

البرهان : (أ) لجميع $(a,b),(c,d) \in R \otimes S$

$$\varphi((a,b)+(c,d))=\varphi(a+c,b+d)=a+c=\varphi(a,b)+\varphi(c,d)$$

$$\varphi((a,b).(c,d))=\varphi(ac,bd)=ac=\varphi(a,b)\varphi(c,d)$$

(ب) لجميع $a,b\in R$

φ هومومورفيزم
$$\left.\begin{array}{l}\varphi(a+b)=(a+b,0)=(a,0)+(b,0)=\varphi(a)+\varphi(b)\\ \varphi(ab)=(ab,0)=(a,0).(b,0)=\varphi(a).\varphi(b)\end{array}\right\rangle$$

φ واحد لواحد $\varphi(a)=\varphi(b)\Rightarrow(a,0)=(b,0)\Rightarrow a=b\Rightarrow$

(جـ) نعرف الراسم

$$\begin{array}{c}\varphi:R\otimes S\to S\otimes R\\ (r,s)\mapsto(s,r)\end{array}$$

لجميع $(r_1,s_1),(r_2,s_2)\in R\otimes S$:

$$\varphi((r_1,s_1)+(r_2,s_2))=\varphi(r_1+r_2,s_1+s_2)=(s_1+s_2,r_1+r_2)$$
$$=(s_1,r_1)+(s_2,r_2)=\varphi(r_1,s_1)+\varphi(r_2,s_2)$$
$$\varphi((r_1,s_1).(r_2,s_2))=\varphi(r_1r_2,s_1s_2)=(s_1s_2,r_1r_2)=(s_1,r_1).(s_2,r_2)$$
$$=\varphi(r_1,s_1).\varphi(r_2,s_2)$$

أى أن φ هومومورفيزم

والآن نعرف الراسم العكسى

$$\begin{array}{c}\psi:S\otimes R\to R\otimes S\\ (s,r)\mapsto(r,s)\end{array}$$

$$\begin{array}{c}\psi o\varphi:R\otimes S\to R\otimes S\\ (r,s)\mapsto(r,s)\end{array}\qquad(1)$$

$$\begin{array}{c}\varphi o\psi:S\otimes R\to S\otimes R\\ (s,r)\mapsto(s,r)\end{array}\qquad(2)$$

(1) تعنى أن $\psi o\varphi=1_{R\otimes S}$ أى راسم الوحدة على $R\otimes S$

(2) تعنى أن $\varphi o \psi = 1_{S \otimes R}$ أى راسم الوحدة على $S \otimes R$

من (1) φ راسم واحد لواحد ، ψ راسم شامل (غامر ، فوقى)

من (7) ψ راسم واحد لواحد ، φ راسم شامل (غامر ، فوقى)

إذن φ (وكذلك ψ) تناظر أحادى وبالتالى φ أيزومورفيزم .

تمارين

(١) اوجد جميع الهومومورفيزمات $\varphi : \mathbb{Z} \otimes \mathbb{Z} \to \mathbb{Z}$

(إرشاد : يتعين الهومومورفيزم – كما نعلم – من معرفة قيمته عند المولدات ، هنا عند (1, 0) ، (0, 1). لاحظ أن φ المعرف كالآتى :

$$\varphi(1,0) = 1 \quad , \quad \varphi(0,1) = 1$$

لن يكون هومومورفيزماً ، لأنه بفرض أن φ هومومورفيزم :

$$\varphi(1,1) = \varphi((1,0) + (0,1)) = \varphi(1,0) + \varphi(0,1) = 1 + 1 = 2,$$
$$\varphi(1,1) = \varphi((1,1).(1,1)) = \varphi(1,1)\varphi(1,1) = (1)(1) = 1$$

وأكمل ...)

(٢) عين جميع الهومومورفيزمات $\varphi : \mathbb{Z} \otimes \mathbb{Z} \to \mathbb{Z} \otimes \mathbb{Z}$

(إرشاد : كما سبق يتعين الهومومورفيزم هنا بمعرفة قيمته عند (1, 0) ، (0, 1) .

هناك تسعة هومومورفيزمات !)

(٣) عين حلقة جزئية من الحلقة $\mathbb{Z} \otimes \mathbb{Z}$ بحيث لاتكون هذه الحلقة الجزئية مثالياً فى $\mathbb{Z} \otimes \mathbb{Z}$

(٤) عين جميع المثاليات فى $\mathbb{Z} \otimes \mathbb{Z}$

(٥) ليكن D_1 ، D_2 نطاقين متكاملين . برهن أو انف :

$D_1 \otimes D_2$ نطاق متكامل .

(٦) اوجد مثالياً أعظم فى $\mathbb{Z} \otimes \mathbb{Z}$ ، مثالياً أولياً فى $\mathbb{Z} \otimes \mathbb{Z}$ ، لكنه ليس أعظم ، مثالياً فعلياً غير أولى فى $\mathbb{Z} \otimes \mathbb{Z}$.

(إرشاد : فى الحلقة المعطاة أى مثالى على الشكل $p\mathbb{Z}\otimes\mathbb{Z}$ حيث p عدد أولى سيكون أعظم . بالمثل $p\mathbb{Z}\otimes q\mathbb{Z}$ حيث p ، q عددان أوليان . أى مثالى على الشكل $p\mathbb{Z}\otimes\{0\}$ حيث p عدد أولى سيكون مثالياً أولياً ، لكنه ليس أعظم .كذلك المثالى $\mathbb{Z}\otimes\{0\}$ أولى لكنه ليس أعظم. أى مثالى على الشكل $n\mathbb{Z}\otimes\{0\}$ حيث n ليس عدداً أولياً هو مثالى فعلى غير أولى . اكتب التفاصيل)

(٧) لتكن $R=\mathbb{Z}_8\otimes\mathbb{Z}_{30}$. اوجد جميع المثاليات العظمى فى R . ومع كل مثالى أعظم I اوجد عدد عناصر الحقل R/I

(٨) عين القواسم الصفرية فى $\mathbb{Z}\otimes\mathbb{Q}\otimes\mathbb{Z}$

(٩) اوجد جميع الوحدات ، القواسم الصفرية ، العناصر المتماثلة القوة ، والعناصر منعدمة القوة فى $\mathbb{Z}_3\otimes\mathbb{Z}_6$.

(١٠) برهن على أن العناصر غير الصفرية فى $\mathbb{Z}_3[i]$ تكون زمرة إبدالية ذات ثمانية عناصر . هل هذه الزمرة تتشاكل مع $\mathbb{Z}_8$ ؟ $\mathbb{Z}_4\otimes\mathbb{Z}_2$ ؟ $\mathbb{Z}_2\otimes\mathbb{Z}_2\otimes\mathbb{Z}_2$ ؟

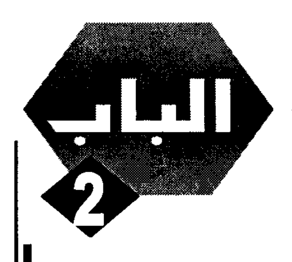
(١١) فى $\mathbb{Z}\otimes\mathbb{Z}$ ليكن $I=\{(a,0)\mid a\in\mathbb{Z}\}$. برهن على أن I مثالى أولى لكنه ليس مثالياً أعظم .

(١٢) هل يمكن لحلقة ذات عنصر الوحدة أن تحتوى فى نفس الوقت على حلقتين جزئيتين تتشاكلان مع $\mathbb{Z}_m$ ، $\mathbb{Z}_n$ حيث $m\neq n$ ؟ وهل يمكن لحلقة ذات عنصر الوحدة أن تحتوى فى نفس الوقت على حلقتين جزئيتين تتشاكلان مع الحلقين $\mathbb{Z}_p$ ، $\mathbb{Z}_q$ حيث p ، q عددان أوليان مختلفان .

(إرشاد : تذكر $\mathbb{Z}_2\otimes\mathbb{Z}_3$)

2 Ring Theory نظرية الحلقات

القسم



حلقات كثيرات الحدود Polynomial Rings

٢ حلقات كثيرات الحدود Polynomial Rings

فى هذا الباب سنجعل كل حلقاتنا لها عنصر الوحدة ، وهى إبدالية ، وسيرسم أى هومومورفيزم حلق عنصر الوحدة فى الحلقة النطاق إلى عنصر الوحدة فى الحلقة النطاق المصاحب (الحلقة الهدف)

لتكن a_0 ، a_1 ، ... ، a_n عناصر حلقة R ، نسمى التعبير الشكلى :

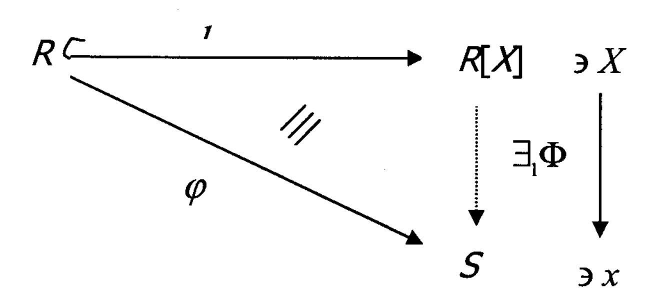
$$f = a_0 + a_1X + ... + a_nX^n$$

كثيرة حدود. تسمى العناصر a_0 ، a_1 ، ... ، a_n معاملات f ، X "غير محدد" حيث يمكن التعويض عن X بأى شىء له معنى .

٢-١ إنشاء حلقات كثيرات الحدود

٢-١-١ تعريف :

لتكن R حلقة . الثلاثى $(R[X], X, \iota)$ المكون من حلقة $R[X]$ ، عنصر "متميز" $X \in R[X]$ ، هومومورفيزم $\iota : R \to R[X]$ يسمى حلقة كثيرة حدود على R فى غير المحدد X عندما تتحقق الخاصة الكونية (العالمية) (universal) : لكل حلقة S ، ولكل $x \in S$ ، ولكل هومومورفيزم $\varphi : R \to S$ ، يوجد **بالضبط هومومورفيزم واحد** $\Phi : R[X] \to S$ بحيث يكون $\Phi(X) = x$ ، ويكون الشكل الآتى إبداليا (commutative)



٢-١-٢ نظرية :

المسألة الكونية (العالمية) فى (٢-١-١) لها حل : $(R[X], X, \iota)$.

ι راسم أحادى (واحد لواحد) بحيث يمكن اعتبار R حلقة جزئية من $R[X]$ ، ولكل $f \in R[X] \setminus \{0\}$ توجد عناصر محددة تماماً $a_0, a_1, ..., a_n \in R$ ، بحيث إن $a_n \neq 0$ ، $n \in \mathbb{N}$ ، $f = a_0 + a_1 X + ... + a_n X^n$.

<u>البرهان</u> : لتكن $R[X]$ حلقة جميع المتواليات $(a_0, a_1, a_2, ...)$ من عناصر فى R حيث $a_k = 0$ لمعظم $k \in \mathbb{N}$. الجمع والضرب فى $R[X]$ يتمان بالطريقة الآتية :

$$(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) := (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...),$$
$$(a_0, a_1, a_2, ...).(b_0, b_1, b_2, ...) := (c_0, c_1, c_2 ...)$$

حيث $c_n := \sum_{k=0}^{n} a_k b_{n-k}$.

ويمكن التحقق أنه بهذا تكون $R[X]$ حلقة إبدالية ذات عنصر الوحدة $(1, 0, 0, ...)$.

الراسم $\begin{matrix} \iota : R \to R[X] \\ a \mapsto (a, 0, 0, ...) \end{matrix}$ مونومورفيزم لأن :

$$\forall a, b \in R : \iota(a+b) = (a+b, 0, 0, ..., 0) = (a, 0, 0, ..., 0) + (b, 0, 0, ..., 0) = \iota(a) + \iota(b)$$
$$\iota(ab) = (ab, 0, 0, ..., 0) = (a, 0, 0, ..., 0).(b, 0, 0, ..., 0) = \iota(a).\iota(b)$$
$$\iota(a) = \iota(b) \Rightarrow (a, 0, 0, ..., 0) = (b, 0, 0, ..., 0) \Rightarrow a = b$$

ولأن ι مونومورفيزم فيمكن أن نوحد (identify) بين R ، صورتها فى $R[X]$.

وليكن العنصر غير المحدد X (ideterminate) هو $X := (0, 1, 0, 0, ...)$ ومن تعريف الضرب فى $R[X]$ نحصل على :

$$X^k = (0, 0, ..., 0, 1, 0, ...) \quad ، \quad k \in \mathbb{N}$$

↑

الموقع رقم k (البداية فى الموقع رقم 0)

وبهذا يكون :

$$\forall f \in R[X] : f := (a_0, a_1, ..., a_n, 0, ...) = a_0 + a_1 X + ... + a_n X^n$$

وواضح أن هذا التمثيل وحيد عندما $f \neq 0$ ، $a_n \neq 0$.

وبمساعدة هذا التمثيل نستطيع أن نبرهن على صحة الخاصة الكونية (العالمية) :

ليكن $\varphi : R \to S$ ، $x \in S$ ، $f = a_0 + a_1X + ... + a_nX^n$

لأن الشكل إبدالى فيجب أن يكون $\Phi(a) = \varphi(a)$ لكل $a \in R$ ، كما أنه بالفرض يجب أن يكون $\Phi(X) = x$. كما أن Φ يجب أن تكون هومومورفيزماً وبالتالى فإن :

$$\Phi(f) = \Phi(a_0 + a_1X + ... + a_nX^n)$$

$$= \Phi(a_0) + \Phi(a_1)\Phi(X) + ... + \Phi(a_n)\Phi(X^n)$$

$$= \Phi(a_0) + \Phi(a_1)\Phi(X) + ... + \Phi(a_n)\Phi(X)^n$$

$$= \varphi(a_0) + \varphi(a_1)x + ... + \varphi(a_n)x^n \qquad (*)$$

وهذا يعنى أنه <u>**يوجد على الأكثر مثل هذا**</u> الهومومورفيزم Φ .

ونثبت الآن أنه يوجد بالفعل مثل هذا الهومومورفيزم ، بأن نعرف Φ كما فى (*) ونثبت أنها بالفعل هومومورفيزم كالآتى :

$$\forall f = a_0 + a_1X + ... + a_nX^n, g = b_0 + b_1X + ... = b_mX^m \in R[X]:$$

$$\Phi(f+g) = \Phi(a_0 + b_0 + (a_1 + b_1)X + ... + (a_n + b_n)X^n + ... + b_mX^m)$$

(بدون فقد للعمومية (without any loss of generality) افترضنا أن $m > n$)

$$\underset{(*)}{=} \varphi(a_0 + b_0) + \varphi(a_1 + b_1)x + ... + \varphi(a_n + b_n)x^n + ... + \varphi(b_m)x^m$$

$$= \quad \varphi(a_0) + \varphi(b_0) + (\varphi(a_1) + \varphi(b_1))x + ... + (\varphi(a_n) + \varphi(b_n))x^n + ... + \varphi(b_m)x^m$$

φ هومومورفيزم

$$= \varphi(a_0) + \varphi(a_1)x + ... + \varphi(a_n)x^n + \varphi(b_0) + \varphi(b_1)x + ... + \varphi(b_n)x^n + ... + \varphi(b_m)x^m$$

$$\underset{(*)}{=} \Phi(f) + \Phi(g)$$

$$\Phi(fg) = \Phi((a_0 + a_1X + ... + a_nX^n)(b_0 + b_1X + ... + b_nX^n + ... b_mX^m))$$

$$= \Phi(a_0b_0 + (a_0b_1 + a_1b_0)X + ... + a_nb_mX^{n+m})$$

$$\underset{(*)}{=} \varphi(a_0b_0) + \varphi(a_0b_1 + a_1b_0)x + ... + \varphi(a_nb_m)x^{n+m}$$

$$= \quad \varphi(a_0)\varphi(b_0)+\varphi(a_0)\varphi(b_1)x+\varphi(a_1)\varphi(b_0)x+\ldots+\varphi(a_n)x^n\varphi(b_m)x^m$$

φ هومومورفيزم

$$=(\varphi(a_0)+\varphi(a_1)x+\ldots+\varphi(a_n)x^n)(\varphi(b_0)+\varphi(b_1)x+\ldots+\varphi(b_m)x^m)$$

$$=\Phi(f)\Phi(g)$$

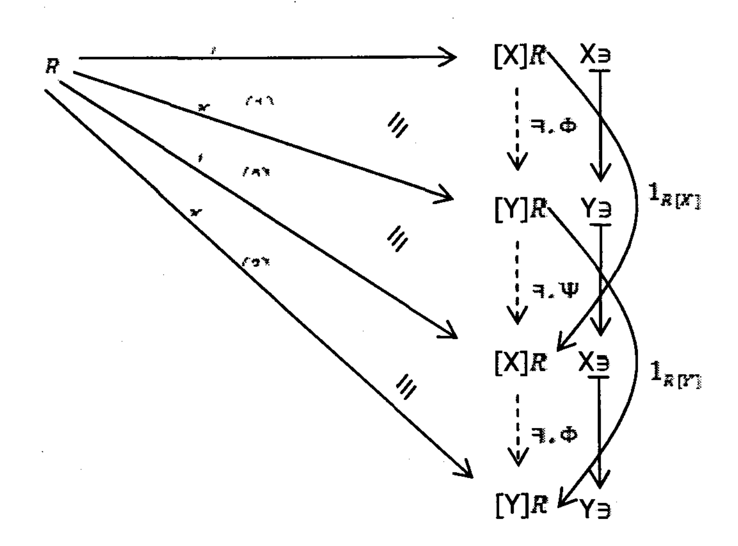
كذلك بالتعريف $\Phi(1)=\varphi(1)$. وبالتالى فإن Φ هومومورفيزم .

<u>٢-١-٣ نظرية</u> :

الحل المعطى فى النظرية (٢-١-٢) وحيد بدون حساب الأيزومورفيزمات (a part from isomorphism)

<u>البرهان</u> :

ليكن لدينا الحلان $(R[X],X,\iota)$ ، $(R[Y],Y,\kappa)$



فى "شبه المثلث" (1) : $R[Y]$ هى الحلقة S ، Y هى العنصر x ، κ هى φ ، $R[X]$ هو حل المسألة . إذن يوجد بالضبط هومومورفيزم وحيد Φ بحيث يجعل "شبه المثلث" (1) إبداليا ، ويرسم X فى Y ، وينتج أن :

$$\Phi o \iota = \kappa \qquad (1)$$

وفى "شبه المثلث" (2) : $R[X]$ هى الحلقة S ، X هى العنصر x ، ι هى φ ، $R[Y]$ هى حل المسألة ، فيوجد بالضبط هومومورفيزم وحيد ψ يجعل "شبه المثلث" (2) إبدالياً ، ويرسم Y فى X وينتج أن

$$\psi o \kappa = \iota \qquad (2)$$

وفى "شبه المثلث" (3) : مرة أخرى $R[Y]$ هى الحلقة S ، X هى العنصر x ، κ هى φ، $R[X]$ هو حل المسألة، فيوجد بالضبط هومومورفيزم وحيد ، هو نفس Φ السابق بالضرورة ، يجعل "شبه المثلث" (3) إبدالياً ، ويرسم X فى Y ، وينتج أن

$$\Phi o \iota = \kappa \qquad (3)$$

من (1) ، (2) ، (3) ينتج أن

$$\iota = \psi o \Phi o \iota \qquad (4)$$

$$\kappa = \Phi o \psi o \kappa \qquad (5)$$

(4) تعنى أن "شبه المثلث" المكون من شبهى المثلثين (1) ، (2) إبدالى . ولكن راسم الوحدة $1_{R[X]}$ وهو هومومورفيزم حلق يجعل نفس شبه المثلث إبدالياً،(ويرسم X فى X) ، ومن حيث إن Φ ، ψ وحيدان فلابد أن يكون $\psi o \Phi$ وحيداً ، وبالتالى يكون

$$\psi o \Phi = 1_{R[X]} \qquad (6)$$

وبالمثل يثبت أن :

$$\Phi o \psi = 1_{R[Y]} \qquad (7)$$

من (6) : Φ راسم واحد لواحد (أحادى) ، ψ راسم غامر (شامل ، فوقى)

من(7) : Φ راسم غامر (شامل ، فوقى) ، ψ راسم واحد لواحد (أحادى)

وكل من Φ ، ψ هومومورفيزم . إذن كلاهما أيزومورفيزم (تشاكل) ، وكل منهما معكوس الآخر . ويكون الحل وحيداً بدون حساب الأيزومورفيزمات (التشاكلات)

<u>ملحوظة</u> : للاختصار كتبنا $R[X]$ هى حل المسألة ولم نكتب $(R[X], X, \iota)$ ، وهكذا ...

٢-١-٤ تعريف :

لتكن R حلقة إبدالية ذات عنصر الوحدة ،

$$f=\sum_{i\in\mathbf{N}} a_i X^i \in R[X]$$

تعرف درجة (f) $(\deg(f))$ بأنها :

$$\deg(f):=\begin{cases}\max\{i\in\mathbb{N}: a_i\neq 0\}, & f\neq 0\\ -\infty & , \quad f=0\end{cases}$$

فى حالة $f\neq 0$ يسمى a_n **المعامل المرشد** (**The leading coefficient**)

وإذا كانت $f\neq 0$ فإنها تسمى "**مطبعة**" (normalized) إذا كان معاملها المرشد هو "1" عنصر الوحدة فى الحلقة .

٢-١-٥ ملحوظة :

لتكن R حلقة إبدالية ، ذات عنصر الوحدة 1 :

(١) $\forall f,g\in R[X]: \deg(fg)\leq \deg(f)+\deg(g)$

(٢) ليكن $0\neq f,g\in R[X]$. المعاملان المرشدان لـــ f ، g كلاهما ليس قاسماً صفرياً لـــ R . عندئذ فإن : $\deg(fg)=\deg(f)+\deg(g)$

(٣) نطاق متكامل $R \Leftrightarrow$ نطاق متكامل $R[X]$

(٤) $(R[X])^*=R^* \Rightarrow$ نطاق متكامل R

البرهان : (١) ، (٢) : ليكن $f,g\in R[X]$. إذا كانت $f=0$ أو $g=0$ فإن $fg=0$ ، وتتحقق المتباينة (١) .

وإذا كانت $f\neq 0$ ، $g\neq 0$ فإنه يوجد $a_0,a_1,\ldots,a_n,b_0,b_1,\ldots,b_n\in R$ بحيث إن $a_m\neq 0\neq b_n$ ، $f=\sum_{i=1}^{m} a_i X^i$ ، $g=\sum_{i=1}^{n} b_i X^i$ ونحصل على : $fg=\sum_{i=1}^{m+n} c_i X^i$

حيث $c_i = \sum_{k+\ell=i} a_k b_\ell$. وينتج مباشرة أن $\deg(fg) \le m+n$ ، وإذا كان $c_{m+n} = a_m b_n \ne 0$ فإن $\deg(fg) = m+n$.

(٣) R ، $R[X]$ كلتاهما حلقة إبدالية ، لهما عنصر الوحدة $0 \ne 1$. فينتج من (١) ، (٢) مباشرة أنه إذا كانت إحداهما نطاقاً متكاملاً كانت الأخرى كذلك .

(٤) واضح أن كل عنصر وحدة فى R سيكون كذلك عنصر وحدة في $R[X]$ ، أى أن $R^* \subset (R[X])^*$. للبرهنة على أن $(R[X])^* \subset R^*$:

لتكن $f \in (R[X])^*$. عندئذ فإنه توجد $g \in R[X]$ بحيث يكون $fg = 1$ ، وبحيث إن $\deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0$.

ومن ثم فإن $\deg(f) = \deg(g) = 0$. وبالتالى فإن $f, g \in R$. ولأن $fg = 1$ فإن $f \in R^*$

<u>**٢-١-٦ نظرية**</u> : خوارزمية القسمة (القسمة مع الباقى)

(Division Algorithm - Division with Remainder)

لتكن R حلقة إبدالية ذات عنصر الوحدة "1"، ولتكن $f, g \ne 0$ كثيرتى حدود فى $R[X]$.

لتكن $m := \deg(f)$ ، $n := \deg(g)$ ، $k := \max\{0, m-n+1\}$.

إذا كان b هو المعامل المرشد لـــ g ، فإنه توجد كثيرتا حدود $q, r \in R[X]$ بحيث يكون :

$$b^k f = qg + r, \deg(r) < \deg(g)$$

إذا لم تكن b قاسماً صفرياً لـــ R فإن q ، r كلتيهما تكون وحيدة .

وإذا كانت b وحدة فى R فإنه يوجد بالضبط q وحيدة ، r وحيدة كلتاهما فى $R[X]$ بحيث يكون :

$$f = qg + r, \deg(r) < \deg(q)$$

<u>**البرهان**</u> : (١) نبرهن بالاستقراء الرياضى على m على أنه يوجد q ، r عنصران فى $R[X]$ بحيث إن $b^k f = qg + r$ ، $\deg(r) < \deg(g)$

إذا كانت $m < n$ فإن $f = 0g + f$ ، ونصل إلى المطلوب مباشرة !

ليكن $m \geq n$ ولنفترض أن الادعاء صحيح لجميع كثيرات الحدود $f \in R[X]$ بحيث إن $\deg(f) \leq m-1$.

لتكن g كثيرة حدود من درجة n ، b هو المعامل المرشد فى g ، a هو المعامل المرشد فى f . عندئذ فإن $\deg(bf - aX^{m-n}g) \leq m-1$ ، ومن فرض الاستقراء توجد كثيرتا حدود $q', r' \in R[X]$ بحيث يكون $\deg(f') \leq m-1$ ،

$$f' = b^{m-1-n+1}(bf - aX^{m-n}g) = q'g + r' \Rightarrow$$

$$(ab^{m-n}X^{m-n} + q')g + r' = b^k f, k = m-n+1$$

(٢) إذا لم تكن b قاسماً صفرياً لـــ R ، وكانت q ، q' ، r ، r' كثيرات حدود فى $R[X]$ بحيث إن : $\deg(r) < \deg(g)$ ، $\deg(r') < \deg(g)$ ، $qg + r = b^k f = q'g + r'$

فإن $(q-q')g = r' - r, \deg(r' - r) < \deg(g)$

ولأن المعامل المرشد لـــ g ليس قاسماً صفرياً لـــ R نحصل على :

$$\deg(r' - r) = \deg(q - q') + \deg(g)$$

$$\Rightarrow q = q', r = r'$$

(٣) إذا كان b وحدة فى R فإنه يوجد $c \in R$ بحيث إن $cb = 1$. وبضرب المتساوية $b^k f = qg + r$ فى c^k نحصل على :

$$f = (c^k q)g + (c^k r)$$

تسمى الحلقات التى يمكن فيها القسمة مع الباقى حلقات إقليدية .

<u>**٢-١-٧ تعريف**</u> :

يقال للزوج (R, d) المكون من نطاق متكامل R ، وراسم $d : R \setminus \{0\} \to \mathbb{N}$ إنه <u>**نطاق إقليدى**</u> (Euclidean domain) إذا كان لكل عنصرين $a, b \in R \setminus \{0\}$ يوجد عنصران $q, r \in R$ بحيث يكون :

(أ) $a = bq + r$

(ب) $d(r) < d(b)$ أو $r = 0$

٢-١-٨ أمثلة :

(١) $(\mathbb{Z},d)$ حيث $\begin{array}{l} d:\mathbb{Z}\setminus\{0\}\to\mathbb{N} \\ n\mapsto |n| \end{array}$ نطاق إقليدى لأن : $\mathbb{Z}$ نطاق متكامل ، الشرطان

(أ)، (ب) فى (٢-١-٧) متحققان . ولكن العنصرين q, r ليسا وحيدين ، فمثلاً

5 = 2.2 + 1 , 5 = 3.2 + (-1)

(٢) ليكن K حقلاً ، وليكن $\begin{array}{l} d:K[X]\setminus\{0\}\to\mathbb{N} \\ f\mapsto \deg(f) \end{array}$. عندئذ فإن الزوج $(K[X],d)$ يكون

نطاقاً إقليدياً (من (٢-١-٥(٣))) $K[X]$ نطاق متكامل، من (٢-١-٦) ، لأن $K^*=K\setminus\{0\}$)

(٣) $\mathbb{Z}[i]:=\{m+in\in\mathbb{C}\,|\,m,n\in\mathbb{Z}\}$ نطاق متكامل . واضح أن $\mathbb{Z}[i]\neq\phi$ ،

$$\forall a+ib, c+id\in\mathbb{Z}[i]: a-c+i(b-d)\in\mathbb{Z}[i],$$
$$ac-bd+i(ad+bc)\in\mathbb{Z}[i]$$

أى أن $\mathbb{Z}[i]$ حلقة جزئية من $\mathbb{C}$. كذلك $\mathbb{Z}[i]$ إبدالية ، ولها عنصر الوحدة $1+i0$ وهو لايساوى $0+i0$. كذلك $\mathbb{Z}[i]$ خالية من القواسم الصفرية لأن $\mathbb{C}$ خالية من القواسم الصفرية ($\mathbb{C}$ حقل !)

يتبقى لكى نثبت أن $\mathbb{Z}[i]$ نطاق إقليدى أن نوجد الراسم d بحيث يحقق الشرطين (أ) ، (ب) فى (٢-١-٧). لهذا نعرف d كالآتى :

$$\begin{array}{l} d:\mathbb{Z}[i]\setminus\{0\}\to\mathbb{N} \\ \quad m+in\mapsto m^2+n^2 \end{array}$$

وإذا كان $\begin{array}{l} d':\mathbb{C}\to\mathbb{N} \\ a+ib\mapsto a^2+b^2 \end{array}$ هو امتداد d (extension) فإننا نلاحظ أن :

$$\forall z,w\in\mathbb{C}: d'(zw)=d'(z)d'(w)$$

لأن : ليكن $z=a+ib$ ، $w=c+id$

$$d'(zw)=d'((a+ib)(c+id))=d'(ac-bd+i(ad+bd))$$
$$=(ac-bd)^2+(ad+bc)^2$$

$$= (a^2 + b^2)(c^2 + d^2) = d'(z)d'(w)$$

والآن إذا كان $z, w \in \mathbb{Z}[i] \setminus \{0\}$ فإنه يوجد $a, b \in \mathbb{R}$ بحيث إن $\frac{z}{w} = a + ib$. والآن

نختار $m, n \in \mathbb{Z}$ بحيث يكون $|a - m| \leq \frac{1}{2}$ ، $|b - n| \leq \frac{1}{2}$ ، فنحصل على :

$$d'(\frac{z}{w} - (m + in)) = (a - m)^2 + (b - n)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

ومن ثم فإن :

$$d(z - (m + in)w) = d(w)d'(\frac{z}{w} - (m + in)) < d(w)$$

ومن حيث إن :

$$z = w(m + in) + (z - (m + in)w)$$
$$= w\, q + r$$

يكون الراسم d حقق الشرطين (أ) ، (ب) . نهاية البرهان .

<u>**٢-١-٩ نظرية :**</u>

إذا كان (R, d) نطاقاً أقليدياً ، فإن R نطاق مثاليات أساسية .

<u>البرهان</u> : واضح أن المثالى $\{0\}$ مثالى أساسى فى R . والآن ليكن $A \subset R$ مثالياً بحيث إن $A \neq \{0\}$. مجموعة جميع العناصر $n \in \mathbb{N}$ بحيث إنه يوجد $a \in A \setminus \{0\}$ ، $d(a) = n$ ليست خالية . ليكن k أصغر عنصر فى هذه المجموعة ، وليكن $a \in A \setminus \{0\}$ بحيث إن $d(a) = k$. واضح أن $[a] \subset A$ (المثالى المتولد من a) .

كذلك فإن $A \subset [a]$ ، لأن : لكل $b \in A$ ، $b \notin [a]$ يوجد $q, r \in R$ بحيث إن : $b = qa + r$ ، $r = 0$ أو $d(r) < d(a) = k$ ، وهذا يستلزم أن $r = b - qa \in A, d(r) < k$ وهذا تناقض مع تعريف k ومن ثم فإن $r = 0$ ، أى أن $b = qa$ وينتج $A \subset [a]$.

وبالتالى فإن $A = [a]$.

نهاية البرهان .

٢-١-١٠ نظرية :

لتكن R حلقة التقريرات الآتية متكافئة :

(١) R حقل

(٢) حلقة كثيرات الحدود $R[X]$ مع الراسم :

$$d : R[X]\setminus\{0\} \to \mathbb{N}$$
$$f \mapsto \deg(f)$$

هى نطاق إقليدى

(٣) $R[X]$ نطاق مثاليات أساسية .

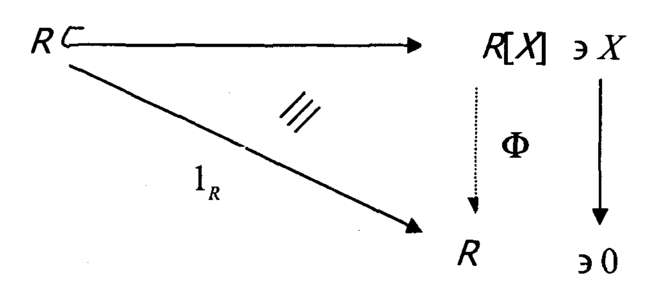
البرهان : "(١) $\Leftarrow$ (٢)" : مثال٢ فى (٢-١-٨)

"(٢) $\Leftarrow$ (٣)" : النظرية (٢-١-٩)

"(٣) $\Leftarrow$ (١)" :

نعتبر الهومومورفيزم : $\Phi : R[X] \to R$, $X \mapsto 0$

الذى يجعل الشكل الآتى إبداليا :



الشكل إبدالى $\Leftarrow$ Φ راسم غامر (شامل)

ومن مثال ٣٦ فى (١-٢-٨) ، ولأن R نطاق متكامل أى لايحتوى على قواسم صفرية فإن R يكون حقلاً إذا كان R يحتوى فقط مثاليات تافهة . ومن مثال ٣٤ فى (١-٢-٨) يكفى أن نبرهن على أنه لايوجد مثالى $A \subset R[X]$ بحيث يكون : $Ker(\Phi) \subsetneq A \subsetneq R[X]$.

ليكن $A \subset R[X]$ مثاليا بحيث إن $Ker(\Phi) \subsetneq A$.

$R[X]$ نطاق مثاليات أساسية $\Leftarrow$ يوجد $f,g\in R[X]$ ، $Ker(\Phi)=[f]$ ، $A=[g]$ ،

$g\notin[f]$. $[f]\subset[g]$ $\Leftarrow$ يوجد $h\in R[X]$: $f=gh$. $f\in Ker(\Phi)\Rightarrow f(0)=0$ ،

لأنه إذا كان $f(0)\neq 0$ فإن :

$$f=a_0+a_1X+\ldots+a_nX^n\Rightarrow\Phi(f)=\Phi(a_0)+\Phi(a_1).\Phi(X)+\ldots+\Phi(a_n).\Phi(X)^n$$

$$\underset{X\in Ker(\Phi)}{=}\Phi(a_0)+\Phi(a_1).0+\ldots+\Phi(a_n).0$$

$$=\Phi(a_0),$$

ولأن الشكل إبدالى فإن $\Phi(a_0)=1_R(a_0)=a_0\neq 0$.

أى أن $\Phi(f)\neq 0$ وهذا يتناقض مع $f\in Ker(\Phi)$. وبالتالى فإن $f(0)=0$.

والآن : $0=f(0)=g(0)h(0)$. $g(0)\neq 0$ وإلا كانت $g\in Ker(\Phi)$ (هذا تناقض مع $g\notin Ker(\Phi)$) . ولأن R نطاق متكامل ، $g(0)\neq 0$ ، فإن $h(0)=0$ ، وهذا يستلزم أن $h\in Ker(\Phi)=[f]$ ومن ثم فإنه يوجد $q\in R[X]$ بحيث إن $h=qf$ ، أى أنه يوجد $q\in R[X]$ بحيث إن : $f=gh=gqf$ ، وهذا يقتضى أنه يوجد $q\in R[X]$ بحيث إن $f(1-gq)=0$. لكن $X\in Ker(\Phi)=[f]$ يعنى أن $f\neq 0$ ولأن R نطاق متكامل ، فإن $1-gq=0$ ، أى أن $gq=1$ ، ومعنى هذا أن g وحدة فى $R[X]$. وبالتالى فإن $A=[g]=R[X]$ (تذكر أنه إذا احتوى المثالى فى حلقة على وحدة، كان المثالى هو الحلقة نفسها) . أى أنه لايوجد مثالى فعلى فى R . نهاية البرهان .

<u>٢-١-١١ نتيجة</u> :

ليكن K حقلاً ، $A\subset R[X]$ مثاليا ، $A\neq\{0\}$. عندئذ فإنه توجد كثيرة حدود مطبعة (normalized polynomial) وحيدة $f\in K[X]$: $A=[f]$.

<u>البرهان</u> :

من (٢-١-١٠) $K[X]$ نطاق مثاليات أساسية ، ومن ثم فإنه يوجد $f\in K[X]\setminus\{0\}$ بحيث إن : $A=[f]$. ولأنه لأى $a\in K^*$: $[af]=[f]$ (واضح !) ، فإنه يمكن اختيار كثيرة الحدود f مطبعة .

والآن إذا كان $f,g\in K[X]$ بحيث إن $[f]=A=[g]$ ، فإنه يوجد $u,v\in K[X]$ بحيث إن : $f=ug$ ، $g=vf$ ومن ثم فإنه يوجد $u,v\in K[X]$ بحيث يكون $f(1-uv)=0$. $K[X]$ نطاق متكامل أى أنه خال من القواسم الصفرية ، ولأن $f\neq 0$ فإن $1-uv=0$ ، وينتج أن $u\in K$ ومن ثم فإن $u=1$ ، $f=g$ عندما تكون f ، g مطبعتين.

٢-٢ أصفار كثيرات الحدود : Zeros of polynomials

٢-٢-١ تعريف :

لتكن R حلقة إبدالية ذات عنصر الوحدة . وليكن $f=\sum_{i=1}^{n} a_iX^i$ كثيرة حدود فى $R[X]$.

يقال لعنصر x فى حلقة تشمل R (superset of R) إنه **صفر** (zero) لـ f إذا كان

$$f(x)=\sum_{i=1}^{n} a_ix^i=0 .$$

٢-٢-٢ تمهيدية :

ليكن R نطاقاً متكاملاً ، $f\in R[X]$ ، $a\in R$ صفر لـ f . عندئذ فإنه توجد كثيرة حدود $g\in R[X]$ بحيث إن $f=(X-a)g$.

البرهان : من (٢-١-٦) توجد كثيرتا حدود $g,r\in R[X]$ بحيث يكون $f=(X-a)g+r$ ، $\deg(r)<\deg(X-a)=1$. ومن ثم فإن r تقع فى R ، بحيث يكون $0=f(a)=r$ ، ينتج أن: $f=(X-a)g$.

٢-٢-٣ نظرية :

ليكن R **نطاقاً متكاملاً** عندئذ فإن كل كثيرة حدود غير صفرية (أى لاتساوى الصفر) f فى $R[X]$ لها على الأكثر $\deg(f)$ من الأصفار .

البرهان : بالاستقراء الرياضى مع الاستعانة بالتمهيدية (٢-٢-٢) .

إذا كانت $f\in R[X]$ لها الدرجة 0 ، فإن $f\in R\setminus\{0\}$ ، ومن ثم فإن f ليس لها أية أصفار.

ليكن $n \in \mathbb{N}$ ، ولتكن كل كثيرة حدود $g \in R[X] \setminus \{0\}$ ، لها الدرجة $\deg(g) \le n$ لها على الأكثر $\deg(g)$ من الأصفار . إذا كانت f من الدرجة $n+1$ ، ولم يكن لها أية أصفار نكون قد انتهينا ! أما إذا كانت f لها الصفر $a \in R$ ، فإنه توجد $g \in R[X]$ بحيث تكون $f=(X-a)g$. ولأن R نطاق متكامل فإن $\deg(f)=\deg(X-a)+\deg(g)$ ، أى أن $\deg(g)=n$ ، وكل صفر لـــ f يختلف عن a هو صفر لـــ g ، وكل صفر لـــ g هو صفر لـــ f . لكن من فرض الاستقراء g لها n من الأصفار على الأكثر ، ومن ثم فإن f لها $n+1$ من الأصفار على الأكثر .

<u>٢-٢-٤ نتيجة</u> :

ليكن R حقلاً ، $a_1,...,a_n \in K$ كلها مختلفة ، $b_1,...,b_n \in K$ ، فإنه توجد بالضبط واحدة $f \in K[X]$ بحيث يكون $\deg(f) \le n-1$ ، $f(a_i)=b_i$ لجميع $i \in \{1,...,n\}$.

<u>البرهان</u> : <u>الوحدانية</u> (uniqueness)

ليكن $f,g \in K[X]$ لهما الخصائص المنشودة ، فينتج أن $a_1,...,a_n$ تكون أصفاراً لـــ $f-g$ ، وكذلك فإن $\deg(f-g) \le n-1$ ، ومن النظرية (٢-٢-٣) ينتج مباشرة أن $f-g=0$ أى أن $f=g$

<u>الوجود</u> (Existence)

كثيرة الحدود :

$$f=\sum_{i=1}^{n} b_i \frac{(X-a_1)...(X-a_{i-1})(X-a_{i+1})...(X-a_n)}{(a_i-a_1)...(a_i-a_{i-1})(a_i-a_{i+1})...(a_i-a_n)}$$

تحقق الخصائص المطلوبة . تسمى كثيرة الحدود هذه : "**<u>كثيرة حدود الاستكمال للجرانج</u>**"

(Lagrange's interpolation polynomial)

<u>٢-٢-٥ أمثلة</u> :

(١) كثيرة الحدود $f := X^2+1 \in \mathbb{R}[X]$ ليس لها أصفار فى $\mathbb{R}$ ، لأن $a^2+1 \ge 1$ لجميع $a \in \mathbb{R}$. لكن العددين المركبين i ، $-i$ صفران لها .

(٢) كثيرات الحدود متعددة غير المحددات (Polynomials of several undeterminates)

لها بصفة عامة عدد لانهائي من الأصفار . على سبيل المثال $f := XY \in \mathbb{R}[X, Y]$:

$f(a,0)=0$ لجميع $a \in \mathbb{R}$.

(٣) النظرية (٢-٢-٣) خاطئة إذا كانت R لها قواسم صفرية .

ليكن $a \neq 0$ قاسماً صفرياً فى R . عندئذ فإنه يوجد $b \in R \setminus \{0\}$ بحيث يكون $ab=0$.

كثيرة الحدود $f := aX \in R[X]$ من الدرجة الأولى ، لكن لها الصفرين 0 ، b .

<u>٢-٢-٦ تعريف</u> :

لتكن R حلقة إبدالية لها عنصر الوحدة ، ولتكن $f := \sum_{i=1}^{n} a_i X^i \in R[X]$.

يسمى الراسم

$$\tilde{f} : R \to R$$
$$x \mapsto f(x) = \sum_{i=0}^{n} a_i x^i$$

<u>راسم كثيرة الحدود الخاص بـ f</u>.

<u>٢-٢-٧ ملحوظة</u> :

لتكن R حلقة إبدالية لها عنصر الوحدة ، ولتكن R مكونة من عدد محدود من العناصر a_1 ، ... ، a_n. عندئذ فإن كثيرة الحدود $f := \prod_{i=1}^{n} (X - a_i)$ فى $R[X]$ ليست كثيرة حدود صفرية أى ليست مساوية للصفر ، لكن $\tilde{f}(x) = 0$ لجميع $x \in R$ ، أى أن $\tilde{f} = 0$.

وكما نرى فكثيرات الحدود لا يمكن اعتبارها دوالاً على الإطلاق كما هى الحال فى التحليل (Analysis). لكن إذا كانت R نطاقاً متكاملاً يتكون من عدد لانهائى من العناصر، فإن كثيرتى حدود f ، g تكونان متساويتين إذا كان راسما كثيرتى الحدود $\tilde{f}$ ، $\tilde{g}$ متساويين .

<u>٢-٢-٨ أمثلة محلولة</u> :

<u>مثال ١</u> : ليكن

$$\varphi : \mathbb{Q}[X] \to \mathbb{R}$$
$$f \mapsto f(\pi)$$

طبق نظرية الهومومورفيزم (١-٣-٣)

الحل : ليكن $f := a_0 + a_1X + ... + a_nX^n$ وبالتالى فإن :

$$\varphi(f) = a_0 + a_1\pi + ... + a_n\pi^n$$

$a_0 + a_1\pi + ... + a_n\pi^n = 0$ إذا كان $a_0 = a_1 = ... = a_n = 0$

وبالتالى فإن $Ker(\varphi) = \{0\}$ ، φ راسم أحادى (واحد لواحد)

$$\Rightarrow \quad \mathbb{Q}[X]/\{0\} \cong \varphi(\mathbb{Q}[X])$$

١-٣-٣

ومن حيث إن $\mathbb{Q}[X]/\{0\} \cong \mathbb{Q}[X]$ ينتج أن

$$\mathbb{Q}[X] \cong \varphi(\mathbb{Q}[X])$$

$$X \leftrightarrow \pi$$

حيث $\varphi(\mathbb{Q}[X])$ هى حلقة جميع كثيرات الحدود فى π ذات المعاملات الكسرية (النسبية)

مثال ٢ : حدد إذا ما كانت التقارير الآتية صحيحة أو خاطئة :

(أ) كثيرة الحدود $a_nX^n + ... + a_1X + a_0 \in R[X]$ تساوى الصفر إذا كان وفقط إذا كان $a_i = 0$ ، $i = 0,1,...,n$

(ب) إذا احتوت الحلقة R على قواسم صفرية ، فإن الحلقة $R[X]$ تحتوى على قواسم صفرية.

(جـ) فى الحلقة R إذا كانت $f(X), g(X) \in R[X]$ من الدرجتين 3 ، 4 فإن كثيرة الحدود $f(X)g(X)$ يمكن أن يكون لها الدرجة 8 .

(د) فى الحلقة R إذا كانت $f(X), g(X) \in R[X]$ من الدرجتين 3 ، 4 فإن كثيرة الحدود $f(X)g(X)$ تكون دائماً من الدرجة 7 .

الحل: (أ) ، (ب) صحيحتان ، (جـ) ، (د) خاطئتان

لاحظ أن هناك فرقاً بين القولين : كثيرة الحدود تساوى الصفر وهو ما جاء فى (أ) وكون كثيرة الحدود لها صفر مثل $f = X - 2$ لها الصفر 2 .

مثال ٣ : اوجد مجموع وحاصل ضرب $f(X):=\bar{3}X^4+\bar{2}X+\bar{4}$ ، $g(X):=\bar{2}X^3+\bar{4}X^2+\bar{3}X+\bar{2}$ إذا علم أن $f(X),g(X)\in (\mathbb{Z}/5\mathbb{Z})[X]$

الحل :

$$f(X)+g(X)=\bar{3}X^4+2X^3+\bar{4}X^2+\bar{5}X+\bar{6}$$
$$=\bar{3}X^4+\bar{2}X^3+\bar{4}X^2+\bar{1}\ (\bar{0}=\bar{5})$$

$$f(X).g(X)=\bar{6}X^7+\overline{12}X^6+\bar{9}X^5+\bar{6}X^4+\bar{4}X^4+\bar{8}X^3+\bar{6}X^2+\bar{4}X+\bar{8}X^3$$
$$+\overline{16}X^2+\overline{12}X+\bar{8}=X^7+\bar{2}X^6+\bar{4}X^5+X^3+\bar{2}X^2+X+\bar{3}$$

مثال ٤ : إذا كان φ الهومومورفيزم

(أ) $\varphi:(\mathbb{Z}/7\mathbb{Z})[X]\to \mathbb{Z}/7\mathbb{Z}$ ، $X\mapsto \bar{2},\bar{a}\mapsto \bar{a}$ فاحسب $\varphi(X^2+\bar{3})$

(ب) $\varphi:(\mathbb{Z}/7\mathbb{Z})[X]\to \mathbb{Z}/7\mathbb{Z}$ ، $X\mapsto \bar{3},\bar{a}\mapsto \bar{a}$ فاحسب $\varphi((X^4+\bar{2}X)(X^3-\bar{3}X^2+\bar{3}))$

الحل : (أ) $\varphi(X^2+\bar{3})=\bar{2}^2+\bar{3}=\bar{4}+\bar{3}=\bar{7}=\bar{0}$

(ب) $\varphi((X^4+\bar{2}X).(X^3-\bar{3}X^2+\bar{3}))=\varphi(X^4+\bar{2}X).\varphi(X^3-\bar{3}X^2+\bar{3})$

$$=(\overline{81}+\bar{6}).(\overline{27}-\overline{27}+\bar{3})=(\overline{87}).(\bar{3})=(\bar{3}).(\bar{3})=\bar{9}=\bar{2}$$

مثال ٥ : ليكن لدينا الهومومورفيزم
$$\varphi:\mathbb{Q}[X]\to\mathbb{R}$$
$$X\mapsto 5$$
$$a\mapsto a$$
. أوجد 6 عناصر فى نواة (φ)

الحل : تذكر أن $(\varphi$ هومومورفيزم يقتضى أن $\varphi(0)=0$ أى أنه دائماً $0\in Ker(\varphi))$

$\varphi(X-5)=5-5=0$. أى أن $X-5\in Ker(\varphi)$

$\varphi(X^2-25)=5^2-5^2=0$. أى أن $X^2-25\in Ker(\varphi)$

وبالمثل X^3-125 ، X^4-625 ، $X^2+X-30=(X-5)(X+6)$ ،

$X^2-9X+20=(X-5)(X-4)$ ، ... ، كلها تقع فى نواة (φ) .

<u>مثال ٦</u> : تنص نظرية فرمات الصغيرة (Fermat's Little Theorem) على الآتى :

ليكن $a\in\mathbb{Z}$ ، p عدداً أولياً لايقسم a عندئذ فإن p يقسم $a^{p-1}-1$

أى أن : $a^{p-1}\equiv 1(\mathrm{mod}\, p), a\not\equiv 0(\mathrm{mod}\, p)$

استخدم نظرية فرمات الصغيرة لحساب $\varphi(X^{231}+\bar{3}X^{117}-\bar{2}X^{53}+\bar{1})$ حيث

$$\varphi:(\mathbb{Z}/5\mathbb{Z})[X]\to \mathbb{Z}/5\mathbb{Z} \quad \text{(هومومورفيزم)}$$
$$X\mapsto 3, \bar{a}\mapsto \bar{a}$$

<u>الحل</u> :

$$\varphi(X^{231}+\bar{3}X^{117}-\bar{2}X^{57}+\bar{1})=(\bar{3})^{231}+\bar{3}(\bar{3})^{117}-\bar{2}(\bar{3})^{53}+\bar{1}$$

$$=(\bar{3}^4)^{57}(\bar{3})^3+\bar{3}(\bar{3}^4)^{29}(\bar{3})-2(\bar{3}^4)^{13}(\bar{3})+\bar{1}$$

$$\equiv(\bar{1})(\overline{27})+\bar{3}(\bar{1})(\bar{3})-(\bar{2})(\bar{1})(\bar{3})+\bar{1}$$

باعتبار $p=5$ فى نظرية فرمات الصغيرة

$$=\bar{2}+\bar{4}-\bar{6}+\bar{1}\equiv\bar{1}(\mathrm{mod}\,5)$$

<u>مثال ٧</u> : باستخدام نظرية فرمات الصغيرة اوجد جميع أصفار كثيرة الحدود الآتية فى $\mathbb{Z}/5\mathbb{Z}$:

$$f:=\bar{2}X^{219}+\bar{3}X^{74}+\bar{2}X^{57}+\bar{3}X^{44}$$

<u>الحـل</u> : سنأخذ $p=5$. واضح أن $X=\bar{0}$ صفر لكثيرة الحدود . والآن بفرض أن $X\not\equiv 0(\mathrm{mod}\, p)$ وبتطبيق نظرية فرمات نحصل على

$$f=\bar{2}(X^4)^{54}X^3+\bar{3}(X^4)^{18}X^2+\bar{2}(X^4)^{19}X+\bar{3}(X^4)^{11}$$

$$\equiv(\bar{2})(\bar{1})X^3+(\bar{3})(\bar{1})X^2+(\bar{2})(\bar{1})X+(\bar{3})(\bar{1})$$

$$\equiv \bar{2}X^3+\bar{3}X^2+\bar{2}X+\bar{3}\equiv\bar{0}$$

$$\Rightarrow \bar{2}X(X^2+\bar{1})+\bar{3}(X^2+\bar{1})\equiv\bar{0}\Rightarrow(X^2+\bar{1})(\bar{2}X+\bar{3})\equiv\bar{0}$$

$\Rightarrow X^2\equiv-\bar{1}\equiv\bar{4}(\bmod 5)$ أو $\bar{2}X\equiv-\bar{3}\equiv\bar{2}(\bmod 5)$

$\Rightarrow X\equiv 2(\bmod 5)$ أو $X\equiv 3(\bmod 5)$ أو $X\equiv 1(\bmod 5)$

إذن الجذور المطلوبة هى $\bar{0}$ ، $\bar{1}$ ، $\bar{2}$ ، $\bar{3}$

مثال ٨ : اوجد جميع الوحدات فى $(\mathbb{Z}/7\mathbb{Z})[X]$

الحل : من الملحوظة (٢-١-٥) (٤) الوحدات فى $(\mathbb{Z}/7\mathbb{Z})[X]$ هى نفس وحدات $\mathbb{Z}/7\mathbb{Z}$. لأن : $7\mathbb{Z}$ مثالى أولى فى $\mathbb{Z}$ لأن 7 عدد أولى (مثال (١-٣-٨)) (١) . ومن (١-٣-١٢ (٢)) يكون $7\mathbb{Z}$ مثالياً أعظم فى $\mathbb{Z}$. وبالتالى وحسب النظرية (١-٣-١١) يكون $\mathbb{Z}/7\mathbb{Z}$ حقلاً وتكون وحداته أى وحدات $(\mathbb{Z}/7\mathbb{Z})[X]$ هى جميع عناصر $\mathbb{Z}/7\mathbb{Z}$ ما عدا $\bar{0}$ أى هى : $\bar{1}$ ، $\bar{2}$ ، ... ، $\bar{6}$. ويمكن رؤية $\mathbb{Z}/7\mathbb{Z}$ حقلاً بطريقة أخرى : رأينا أن $7\mathbb{Z}$ مثالى أولى فى $\mathbb{Z}$ وحسب (١-٣-٩) يكون $\mathbb{Z}/7\mathbb{Z}$ نطاقاً متكاملاً . ولكنه منته (عدد عناصره = 7) فمن (١-١-١٣) يكون $\mathbb{Z}/7\mathbb{Z}$ حقلاً .

مثال ٩ : برهن على أن كثيرة الحدود $X^2+\bar{3}X+\bar{2}$ لها أربعة أصفار فى $(\mathbb{Z}/6\mathbb{Z})[X]$. كيف تفسر هذا على الرغم من أن درجة كثيرة الحدود المعطاة هى 2 ؟

الحل : بالتعويض المباشر نستنتج أن $\bar{1}$ ، $\bar{2}$ ، $\bar{4}$ ، $\bar{5}$ كلها أصفار لكثيرة الحدود المعطاة. ونحن نعلم أن $\mathbb{Z}/6\mathbb{Z}$ ليس نطاقاً متكاملاً لأن $\bar{6}$ ليس عدداً أولياً (مثال (١) فى (١-٣-٨)، (١-٣-٩)) أو من ملاحظة أن :

$$\bar{0}=\bar{2}\bar{3},\quad \bar{2}\neq\bar{0}\neq\bar{3}$$

أى أن $\mathbb{Z}/6\mathbb{Z}$ ليس خالياً من القواسم الصفرية ، وبالتالى ليس نطاقاً متكاملاً ، ومن (٢-١-٥ (٣)) يكون $(\mathbb{Z}/6\mathbb{Z})[X]$ ليس نطاقاً متكاملاً . النظرية (٢-٢-٣) تكون خاطئة حال كون الحلقة المعنية لها قواسم صفرية .

<u>مثال ١٠</u> : ليكن $f(X) := X^3 + \bar{2}X + \bar{4}$ ، $g(X) := \bar{3}X + \bar{2}$ عنصرين فى $(\mathbb{Z}/5\mathbb{Z})[X]$. عين خارج قسمة $f(X)$ على $g(X)$ ، وباقى القسمة .

<u>الحل</u> : نجرى القسمة كالآتى :

$$\begin{array}{r|l} & \bar{2}X^2 + \bar{2}X + \bar{1} \\ \bar{3}X + \bar{2} & X^3 + \bar{2}X + \bar{4} \\ (\bar{2}.\bar{3} = \bar{6} = \bar{1}) & X^3 + \bar{4}X^2 \\ \hline (-\bar{4} = \bar{6}) & \bar{6}X^2 + \bar{2}X + \bar{4} \\ & \bar{6}X^2 + \bar{4}X \\ \hline (-\bar{2} = \bar{3}) & \bar{3}X + \bar{4} \\ & \bar{3}X + \bar{2} \\ \hline & \bar{2} \end{array}$$

أى أن خارج القسمة هو $\bar{2}X^2 + \bar{2}X + \bar{1}$ ، باقى القسمة $\bar{2}$.

<u>مثال ١١</u> : برهن على أن كثيرة الحدود $\bar{2}X + \bar{1} \in (\mathbb{Z}/4\mathbb{Z})[X]$ لها معكوس ضربى فى $(\mathbb{Z}/4\mathbb{Z})[X]$.

<u>البرهان</u> : لاحظ أن : $(\bar{2}X + 1)^2 = \bar{4}X^2 + \bar{4}X + \bar{1} = \bar{1}$

أى أن $\bar{2}X + \bar{1}$ هى معكوس نفسها الضربى فى $(\mathbb{Z}/4\mathbb{Z})[X]$.

<u>مثال ١٢</u> : ليكن F حقلاً غير منته ، $f(X) \in F[X]$ ، إذا كان $f(a) = 0$ لعدد لانهائى من العناصر $a \in F$. برهن على أن $f(X) = 0$.

البرهان : تعلم من النظرية (٢-٢-٣) أنه إذا كان R نطاقاً متكاملاً ، فإن أية كثيرة حدود فى $R[X]$ **وغير صفرية** يكون عدد أصفاها لايزيد على درجتها . وبالتالى إذا كان R حقلاً تكون النظرية صحيحة . ومن حيث إن عدد أصفار الدالة $f(X)$ لانهائى ودرجتها نهائية (finite) ، فلابد أن تكون الدالة صفرية، أى يكون $f(X)=0$.

مثال ١٣ : اوجد كثيرة حدود لها معاملات صحيحة بحيث يكون $\frac{1}{2}$ ، $-\frac{1}{3}$ صفرين لها.

الحل : $\frac{1}{2}$ ، $-\frac{1}{3}$ صفرين لكثيرة الحدود يعنى أن $(X-\frac{1}{2})$ ، $(X+\frac{1}{3})$ عاملان من عواملها . وحتى تكون كل معاملاتها صحيحة تكون كثيرة الحدود المطلوبة هى :

$$f(X)=6(X+\frac{1}{3})(X-\frac{1}{2})=6X^2-X-1$$

مثال ١٤ : ليكن F حقلاً ، ولتكن $f := a_nX^n + a_{n-1}X^{n-1}+\ldots+a_0 \in F[X]$.
برهن على أن $X-1$ عامل من عوامل f إذا كان وفقط إذا كان

$$a_n + a_{n-1}+\ldots+a_0 = 0$$

البرهان : كما رأينا فى التمهيدية (٢-٢-٢) إذا كان $X-1$ عاملاً من عوامل كثيرة الحدود f ، فإنه توجد كثيرة حدود g بحيث يكون $f=(X-1)\,g$.
(بدهى أن $X-a$ عامل من عوامل f بمعنى a صفر لكثيرة الحدود f) وينتج أن $f(1)=0$.
ومن ثم فإن : $a_n + a_{n-1}+\ldots+a_0 = 0$
وبالعكس إذا كان $a_n+a_{n-1}+\ldots+a_0=0$ فإن $f(1)=0$ وبالتالى فإن $X-1$ عامل من عوامل f .

مثال ١٥ : إذا كان m عدداً صحيحاً موجباً، ولأى عدد صحيح a ، ليكن $\bar{a} := a(\mathrm{mod}\, m)$
برهن على أن الراسم

$$\varphi:\mathbb{Z}[X]\to(\mathbb{Z}/m\mathbb{Z})[X]$$
$$a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0 \mapsto \bar{a}_nX^n+\bar{a}_{n-1}X^{n-1}+\ldots+\bar{a}_0$$

هومومورفيزم حلق

البرهان : واضح أن φ معرف جيداً ، كما أن $\varphi(1)=\bar{1}$

$$\forall a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0, b_mX^m+b_{m-1}X^{m-1}+\ldots+b_0\in\mathbb{Z}[X], m\ge n:$$

$$\varphi(a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0+b_mX^m+b_{m-1}X^{m-1}+\ldots+b_0)$$

$$=\varphi(b_mX^m+b_{m-1}X^{m-1}+\ldots+(a_n+b_n)X^n+(a_{n-1}+b_{n-1})X^{n-1}+\ldots+a_0+b_0)$$

$$=\bar{b}_mX^m+\bar{b}_{m-1}X^{m-1}+\ldots+(\overline{a_n+b_n})X^n+(\overline{a_{n-1}+b_{n-1}})X^{n-1}+\ldots+\bar{a}_0+\bar{b}_0$$

$$=\bar{b}_mX^m+\bar{b}_{m-1}X^{m-1}+\ldots+\bar{b}_0+\bar{a}_nX^n+\bar{a}_{n-1}X^{n-1}+\ldots+\bar{a}_0$$

$$=\varphi(a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0)+\varphi(b_mX^m+b_{m-1}X^{m-1}+\ldots+b_0).$$

$$\varphi((a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0)(b_mX^m+b_{m-1}X^{m-1}+\ldots+b_0))$$

$$=\varphi(a_nb_mX^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)X^{n+m-1}+\ldots+a_0b_0)$$

$$=\overline{a_nb_m}X^{n+m}+(\overline{a_nb_{m-1}+a_{n-1}b_m})X^{n+m-1}+\ldots+\overline{a_0b_0}$$

$$=(\bar{a}_nX^n+\bar{a}_{n-1}X^{n-1}+\ldots+\bar{a}_0)(\bar{b}_mX^m+\bar{b}_{m-1}X^{m-1}+\ldots+\bar{b}_0)$$

$$=\varphi(a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0)\varphi(b_mX^m+b_{m-1}X^{m-1}+\ldots+b_0)$$

$$\varphi(1)=\bar{1}$$

أى أن φ هومومورفيزم

مثال ١٦ : لكل عدد صحيح $p>1$ ، برهن على أن : $(p-1)!\equiv-1(\mathrm{mod}\, p)$

إذا كان وفقط إذا كان p عدداً أولياً (نظرية ويلسون Wilson's Theorem)

البرهان : ليكن K حقلاً منتهياً . عندئذ فإن : $\prod_{a\in K^*} a=-1$ ، لأن :

نعتبر المجموعة M المعرفة كالآتى :

$$M:=\{a\in K^*\mid a=a^{-1}\}$$
$$=\{a\in K^*\mid a^2=1\}$$

واضح أن : $\prod_{a\in M} a=\prod_{a\in K^*} a$

العنصر $a\in K$ يقع فى M إذا كان وفقط إذا كان a صفراً لكثيرة الحدود $X^2-1\in K[X]$. وكثيرة الحدود $X^2-1\in K[X]$ لها صفران فقط هما 1 + ، 1 - .

ومن ثم ينتج أن $\prod_{a\in K^*} a=-1$.

والآن بتطبيق هذا على الحقل $K=\mathbb{Z}/p\mathbb{Z}$ نحصل على :

$$\bar{1}.\bar{2}...\overline{p-1}=\overline{-1}\Rightarrow\overline{1.2....(p-1)}=\overline{-1}$$

أى أن $(p-1)!\equiv -1(\bmod p)$

مثال ١٧ : برهن على أنه لأى عدد أولى p :

$$(p-2)!\equiv 1(\bmod p)$$

البرهان : من مثال ١٦ السابق مباشرة (نظرية ويلسون) لدينا :

$$(p-1).(p-2)!\equiv -1(\bmod p)$$
$$\Rightarrow \exists k\in\mathbb{N}:[(p-1).(p-2)!+1]=pk$$
$$\Rightarrow \exists k\in\mathbb{N}:p.(p-2)!-(p-2)!=-1+pk$$
$$\Rightarrow \exists k\in\mathbb{N}:(p-2)!=p[-k+(p-2)!]+1$$
$$\Rightarrow (p-2)!\equiv 1(\bmod p)$$

مثال ١٨ : برهن على أن $(50!)^2\equiv -1(\bmod 101)$

البرهان :

$$(50!)^2=(50!)(-1)(-2)...(-50)$$
$$\equiv(50!)(100)(99)...(51)(\bmod 101)$$
$$\equiv(100)!(\bmod 101)\equiv -1(\bmod 101)$$

مثال ١٩ : لتكن $\mathbb{R}\{X\}$ حلقة كثيرات الحدود ذات المعاملات الحقيقية . وليكن $[X^2+1]$ هو المثالى (الرئيسى) المتولد من كثيرة الحدود X^2+1 ، أى أن :

$$[X^2+1]=\{f:(X^2+1) \mid f\in\mathbb{R}[X]\}$$

عندئذ فإن :

$$\mathbb{R}[X]\Big/_{[X^2+1]}=\{g+[X^2+1]\}=\{aX+b+[X^2+1] \mid a,b\in\mathbb{R}\}$$

لأنه إذا كانت g أية كثيرة حدود فى $\mathbb{R}[X]$ فإننا نستطيع أن نكتب $g=q(X^2+1)+r$ حيث q هى خارج القسمة ، r باقى القسمة عندما نقسم كثيرة الحدود g على X^2+1. وعلى وجه الخصوص $r=0$ أو $\deg(r)<2$ أى أن $r=aX+b$ حيث $a,b\in\mathbb{R}$ وهكذا فإن :

$$g+[X^2+1]=q(X^2+1)+r+[X^2+1]=r+[X^2+1]$$

لأن المثالى $[X^2+1]$ "يمتص" الحد $q(X^2+1)$.

ونلاحظ أن

$$X^2+1+[X^2+1]=0+[X^2+1]$$

وعلى سبيل المثال فإن :

$$\begin{aligned}
&(X+3+[X^2+1]).(2X+5+[X^2+1])\\
&=2X^2+11X+15+[X^2+1]\\
&=2(X^2+1)+11X+13+[X^2+1]\\
&=11X+13+[X^2+1]
\end{aligned}$$

مثال ٢٠ : برهن على أن :

$$\mathbb{Q}[X]\Big/_{[X^2-2]}\cong\mathbb{Q}[\sqrt{2}]:=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$$

البرهان : نعرف الراسم

$$\varphi:\mathbb{Q}[X]\to\mathbb{Q}[\sqrt{2}]$$
$$p\mapsto p(\sqrt{2})$$

φ هومومورفيزم :

$$\forall p,q \in \mathbb{Q}[X] : \varphi(p+q) = (p+q)(\sqrt{2}) = p(\sqrt{2}) + q(\sqrt{2}) = \varphi(p) + \varphi(q)$$

$$\varphi(p.q) = (p.q)(\sqrt{2}) = p(\sqrt{2}).q(\sqrt{2}) = \varphi(p).\varphi(q)$$

$$\varphi(1) = 1$$

φ غامر (شامل) : لكل $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ يوجد $a + bX \in \mathbb{Q}[X]$:

$$\varphi(a+bX) = a + b\sqrt{2}$$

نحسب نواة (φ)

$$Ker(\varphi) := \{p \in \mathbb{Q}[X] \mid p(\sqrt{2}) = 0\}$$

نبرهن على أن

$$Ker(\varphi) = [X^2 - 2]$$

واضح أن $[X^2 - 2] \subset Ker(\varphi)$ لأن $\varphi(X^2 - 2) = 2 - 2 = 0$

نبرهن على أن $Ker(\varphi) \subset [X^2 - 2]$: ليكن $p \in Ker(\varphi)$ بالقسمة الإقليدية نحصل على :

$$p = q(X^2 - 2) + rX + s$$

حيث $q \in \mathbb{Q}[X]$ ، $r, s \in \mathbb{Q}$

($rX + s$ هو باقى قسمة p على $X^2 - 2$ ويجب أن تكون درجته هى الأولى)

(لأن $p \in Ker(\varphi)$) $\Rightarrow p(\sqrt{2}) = q.0 + r\sqrt{2} + s = 0$

$$\Rightarrow r = 0, s = 0$$

$$\Rightarrow p = q(X^2 - 2), q \in \mathbb{Q}[X]$$

أى أن $Ker(\varphi) \subset [X^2 - 2]$

نطبق نظرية الهومومورفيزم فنحصل على

$$\mathbb{Q}[X] / [X^2 - 2] = \mathbb{Q}[X] / Ker(\varphi) \cong \varphi(\mathbb{Q}[X]) = \mathbb{Q}[\sqrt{2}]$$

φ غامر

نهاية البرهان

مثال ٢١ : اضرب مثالاً لحلقة إبدالية ذات عنصر وحدة R ، I مثالى أعظم فيها ، بحيث إن $I[X]$ ليس مثالياً أعظم فى $R[X]$.

الحل : خذ الحلقة $\mathbb{Z}$ ، المثالى $I=[2]$ أى $2\mathbb{Z}$ مثالى أعظم فى $\mathbb{Z}$ (من (١-٣-٨ (١)) $2\mathbb{Z}$ مثالى أولى فى $\mathbb{Z}$ ، من (١-٣-١٢ (٢)) $2\mathbb{Z}$ مثالى أعظم فى $\mathbb{Z}$)

المثالى $I[X]$ يعرف كالآتى :

$$I[X]:=\{f : f := a_0 + a_1X + \ldots + a_nX^n, n \in \mathbb{N}, 2^m \mid a_0, \ldots, a_n, m \in \mathbb{N} \setminus \{0\}\}$$

واضح أن $X \notin I[X]$ ، بينما أن $X \in [2, X]$

يمكن البرهنة كذلك على أن $[2,X] \underset{\neq}{\subset} \mathbb{Z}[X]$. وبالتالى يكون

$$I[X] \underset{\neq}{\subset} [2,X] \underset{\neq}{\subset} \mathbb{Z}[X]$$

مثال ٢٢ : برهن على أن المثالى $[2X]$ ليس مثاليا أعظم فى $\mathbb{Z}[X]$.

البرهان :

$[2X]$ ليس مثاليا أعظم فى $\mathbb{Z}[X]$ ، لأن : $[2,X] \underset{\neq}{\supset} [2X]$ ، فمثلاً $2 \in [2,X]$ ، $2 \notin [2X]$ ، لجميع $z \in [2X]$: $z \in [2,X]$. كذلك فإن $[2,X] \underset{\neq}{\subset} \mathbb{Z}[X]$ ، فمثلاً $1 \in \mathbb{Z}[X]$ ، بينما $1 \notin [2,X]$. إذا كان $1 \in [2,X]$ فإنه يوجد $f, g \in \mathbb{Z}[X]$ بحيث أن $1 = 2.f + X.g$.

ليكن $f := a_0 + a_1X + \ldots + a_nX^n$ ، $g := b_0 + b_1X + \ldots + b_mX^m$ والآن :

$$1 = 2(a_0 + a_1X + \ldots + a_nX^n) + X(b_0 + b_1X + \ldots + b_mX^m)$$

$$\Rightarrow 1 = 2a_0 \Rightarrow a_0 = \frac{1}{2}$$

وهذا تناقض لأن $a_0, \ldots, a_n \in \mathbb{Z}$ (كذلك $b_0, \ldots, a_m \in \mathbb{Z}$)

وبالتالى فإن :

$$[2X] \underset{\neq}{\subset} [2,X] \underset{\neq}{\subset} \mathbb{Z}[X]$$

نهاية البرهان .

مثال ٢٣ : ليكن $f(X)$ عنصراً فى $\mathbb{R}[X]$. إذا كان $f(a)=0$ ، $f'(a)=0$ ($f'(a)$ هو مشتقة الدالة $f(X)$ عند $X=a$) ، فبرهن على أن $(X-a)^2$ قاسم لـــ $f(X)$.

البرهان : من التمهيدية (٢-٢-٢) : $f(a) = 0$ يقتضى أنه توجد كثيرة حدود $g(X)\in \mathbb{R}[X]$ بحيث إن : $f=(X-a)g$. والآن باجراء التفاضل للطرفين بالنسبة إلى X نحصل على :

$$f'=(X-a)g'+g$$

$$\Rightarrow 0=f'(a)=(a-a)g'+g(a)\Rightarrow g(a)=0$$

مرة أخرى من التمهيدية (٢-٢-٢) توجد كثيرة حدود $h(X)\in \mathbb{R}[X]$ بحيث إن : $g=(X-a)h$. ومن ثم فإن : $f=(X-a)^2 h$.

نهاية البرهان .

مثال ٢٤ : برهن على أن المثالى $[X]$ فى $\mathbb{Z}[X]$ أولى ، لكنه ليس أعظم .

البرهان : نعتبر الراسم :

$$\varphi:\mathbb{Z}[X]\to\mathbb{Z}$$
$$f=a_0+a_1X+\ldots+a_nX^n\mapsto a_0$$

واضح أن الراسم معرف جيداً .

φ هومومورفيزم : ليكن $f,g\in\mathbb{Z}[X]$:

$$f:=a_0+a_1X+\ldots+a_nX^n,g:=b_0+b_1X+\ldots+b_mX^m,a_0,\ldots,a_n,b_0,\ldots,b_m\in\mathbb{Z}$$
$$\varphi(f+g)=\varphi(a_0+b_0+(a_1+b_1)X+\ldots+(a_n+b_n)X^n+b_{n+1}X^{n+1}+\ldots+b_mX^m)$$

(بدون فقد للعمومية (without any loss of generality) أخذنا $n<m$)

$$=a_0+b_0=\varphi(f)+\varphi(g)$$

$$\varphi(f.g)=\varphi((a_0+a_1X+\ldots+a_nX^n).(b_0+b_1X+\ldots+b_mX^m))$$

$$=\varphi(c_0+c_1X+\ldots+c_{n+m}X^{n+m}),c_i=\sum_{j=0}^{i}a_jb_{i-j}$$

$$=c_0=a_0b_0=\varphi(f).\varphi(g)$$

كذلك واضح أن $\varphi(1)=1$ (عنصر الوحدة فى $\mathbb{Z}[X]$ هو "1" ، وهو كذلك عنصر الوحدة فى $\mathbb{Z}$) .

أى أن φ هومومورفيزم

واضح أن φ راسم غامر (شامل ، فوقى)

$$Ker(\varphi)=\{f\in\mathbb{Z}[X],f:=a_0+a_1X+...+a_nX^n,a_0,...,a_n\in\mathbb{Z})\mid\varphi(f)=a_0=0\}$$
$$=\{a_1X+a_2X^n+...+a_nX^n\mid a_1,...,a_n\in\mathbb{Z}\}$$
$$=[X]$$

وبتطبيق نظرية الهومومورفيزم (١-٣-٣) فينتج أن :

$$\mathbb{Z}[X]\big/[X]=\mathbb{Z}[X]\big/Ker(\varphi)\quad\cong\quad\varphi(\mathbb{Z}[X])=\mathbb{Z}$$

φ غامر

ولأن $\mathbb{Z}$ نطاق متكامل وليس حقلاً فإنه ينتج من (١-٣-٩) ، (١-٣-١١) أن $[X]$ مثالى أولى فى

$\mathbb{Z}[X]$ وليس مثالياً أعظم فى $\mathbb{Z}[X]$.

<u>مثال ٢٥</u> : برهن على أن أى حقل هو نطاق إقليدى .

البرهان : كل حقل هو نطاق متكامل ، إذن يتبقى البرهنة على أنه يوجد راسم $d:K\setminus\{0\}\to\mathbb{N}$ (K هو الحقل) بالخصائص المعطاة فى (٢-١-٧) . سنعرف d كالآتى :

$$d:K\setminus\{0\}\to\mathbb{N}$$
$$a\mapsto 0$$

ولأى $a,b\in K\setminus\{0\}$ نستطيع أن نكتب :

$$a=ab^{-1}.b$$

وبالمقارنة مع $a=qb+r$ يكون $r=0,q=ab^{-1}$.

نهاية البرهان .

مثال ٢٦ : برهن على أن أى حقل K هو نطاق مثاليات أساسية .

البرهان : من المثال السابق مباشرة نعلم أن أى حقل هو نطاق إقليدى ، ومن النظرية (٢-١-٩) كل نطاق إقليدى هو نطاق مثاليات أساسية ، فينتج المطلوب مباشرة .

طريقة أخرى : نعلم من مثال ٥٢ فى (١-٢-٨) أن الحقل K لايحتوى من المثاليات إلا المثاليين التافهين : $\{0\}$ ، K نفسه . المثالى $\{0\}$ يتولد من 0 ، إذن هو مثالى أساسى . المثالى K يتولد من العنصر "1" لأن :

$$\forall x \in K : x = 1.x \in [1]$$

مثال ٢٧ : اضرب مثالاً لبيان أن مثالياً أولياً فى حلقة إبدالية ذات عنصر الوحدة ليس بالضرورة مثالياً أعظم .

الحـــل : سنأخذ المثالى $[X]$ فى الحلقة $\mathbb{Z}[X]$ ، وسنشير إليه بالرمز I . لتكن $f(X)$ ، $g(X)$ كثيرتى حدود فى الحلقة $\mathbb{Z}[X]$ ، بحيث إن $f(X)g(X) \in I$. من الواضح أن $f(X)g(X) = Xh(X)$ لبعض $h(X) \in \mathbb{Z}[X]$

والآن ليكن :

$$f(X) := a_0 + a_1 X + \dots + a_n X^n, a_n \neq 0,$$

$$g(X) := b_0 + b_1 X + \dots + b_m X^m, b_m \neq 0,$$

$$h(X) := c_0 + c_1 X + \dots + c_p X^p, c_p \neq 0 \ .$$

عندئذ فإن :

$$f(X)g(X) = Xh(X) \Rightarrow$$

$$(a_0 + a_1 X + \dots + a_n X^n)(b_0 + b_1 X + \dots + b_m X^m) = X(c_0 + c_1 X + \dots + c_p X^p)$$

$$\Rightarrow a_0 b_0 = 0 \Rightarrow a_0 = 0 \quad \text{أو} \quad b_0 = 0$$

$$a_0 = 0 \Rightarrow f(X) = a_1 X + a_2 X^2 + \dots + a_n X^n = X(a_1 + a_2 X + \dots + a_n X^{n-1}) \in I$$

وبالمثل $b_0 = 0 \Rightarrow g(X) = b_1 X + b_2 X^2 + \dots + b_m X^m = X(b_1 + b_2 X + \dots + b_m X^{m-1}) \in I$

وهكذا فإن : (1) $f(X)g(X) \in I \Rightarrow f(X) \in I$ أو $g(X) \in I$

وواضح أن $I=[X]\neq \mathbb{Z}[X]$ ، فعلى سبيل المثال $2\in \mathbb{Z}[X]$ ، لكن $2\notin [X]$.
إذا كان $2\in [X]$ فإنه يوجد $h(X)\in \mathbb{Z}[X]$ بحيث أن : $2=h(X)X$ ولأن $\mathbb{Z}[X]$ نطاق متكامل ($\mathbb{Z}$ نطاق متكامل ، (٢-١-٥ (٣))) فإن :

$$\deg(2)=\deg h(X)+\deg(X)$$

وهذا تناقض $\Rightarrow 0>1$

أى أن

$$2\notin [X],2\in \mathbb{Z}[X] \qquad (2)$$

من (1) ، (2) ينتج أن $[X]$ مثالى أولى فى $\mathbb{Z}[X]$.
والآن نبرهن على أن $[X]$ ليس مثاليا أعظم فى $\mathbb{Z}[X]$:
المثالى $[X,2]$ المتولد من X ، 2 يحقق :

$$[X]\subsetneq[X,2]\subsetneq\mathbb{Z}[X]$$

لأن $2\in [X,2]$ ، $2\notin [X]$
كذلك فإن $1\in \mathbb{Z}[X]$ ، $1\notin [X,2]$ (انظر مثال ٢٢ السابق) وبالتالى فإنه $[X]$ ليس مثاليا أعظم فى $\mathbb{Z}[X]$. نهاية البرهان
(قارن مع مثال ٢٤)

<u>مثال ٢٨</u> : برهن على أنه لأى مثالى غير تافه I فى $\mathbb{Z}[i]$ يكون $\mathbb{Z}[i]/I$ منتهيا .

<u>البرهان</u> : نعلم من مثال ٣ فى (٢-١-٨) أن $\mathbb{Z}[i]$ نطاق إقليدى ، ومن ثم فإن من (٢-١-٩) يكون نطاق مثاليات أساسية . وبالتالى فإنه يوجد $a,b\in \mathbb{Z}$ بحيث يكون $I=[a+bi]$. والآن :

$$a^2+b^2+I=(a+bi)(a-bi)+I=I\Rightarrow a^2+b^2\in I$$

والآن لأى $c,d\in \mathbb{Z}$

$$c=q_1(a^2+b^2)+r_1,0\leq r_1<a^2+b^2$$
$$d=q_2(a^2+b^2)+r_2,0\leq r_2<a^2+b^2$$

ومن ثم فإن :

$$c + di + I = q_1(a^2+b^2) + r_1 + iq_2(a^2+b^2) + ir_2 + I$$
$$= r_1 + ir_2 + I$$

أى أن $\mathbb{Z}[i]/I$ منته .

<u>**مثال ٢٩**</u> : إذا كان $\varphi: R \to S$ هومومورفيزم حلق . عرف $\bar{\varphi}: R[X] \to S[X]$ كالآتى :

$$\bar{\varphi}(a_nX^n + \ldots + a_0) = \varphi(a_n)X^n + \ldots + \varphi(a_0)$$

برهن على أن $\bar{\varphi}$ هومومورفيزم حلق . (R, S حلقتان إبداليتان)

<u>**البرهان**</u> :

$$\forall a_nX^n + \ldots + a_0,\ \ b_mX^m + \ldots + b_0 \in R[X]$$

وبدون فقد للعمومية ليكن $n < m$

$$\bar{\varphi}(a_nX^n + \ldots + a_0 + b_mX^m + \ldots + b_0)$$
$$= \quad \bar{\varphi}(b_mX^m + \ldots + (a_n + b_n)X^n + \ldots + b_0 + a_0)$$

$R[X]$ إبدالية

$$= \quad \varphi(b_m)X^m + \ldots + \varphi(a_n + b_n)X^n + \ldots + \varphi(b_0 + a_0)$$

$\bar{\varphi}$ تعريف

$$= \quad \varphi(b_m)X^m + \ldots + \varphi(a_n)X^n + \varphi(b_n)X^n + \ldots + \varphi(b_0) + \varphi(a_0)$$

φ هومومورفيزم

$$= \quad \varphi(a_n)X^n + \ldots + \varphi(a_0) + \varphi(b_m)X^m + \ldots + \varphi(b_0)$$

$R[X]$ إبدالية

$$= \bar{\varphi}(a_nX^n + \ldots + a_0) + \bar{\varphi}(b_mX^m + \ldots + b_0) \qquad (1)$$

$\bar{\varphi}$ تعريف

$$\bar{\varphi}((a_nX^n + \ldots + a_0)(b_mX^m + \ldots + b_0))$$
$$= \bar{\varphi}(a_nb_mX^{n+m} + \ldots + a_0b_0)$$

$R[X]$ إبدالية

$$= \varphi(a_n b_m)(X^{n+m}) + ... + \varphi(a_0 b_0)$$

تعريف $\overline{\varphi}$

$$= \quad \varphi(a_n)\varphi(b_m)X^{n+m} + ... + \varphi(a_0)\varphi(b_0)$$

هومومورفيزم φ

$$= \quad (\varphi(a_n)X^n + ... + \varphi(a_0))(\varphi(b_m)X^m + ... + \varphi(b_0))$$

إبدالية $R[X]$

$$= \overline{\varphi}(a_n X^n + ... + a_0)\overline{\varphi}(b_m X^m + ... + b_0) \qquad (2)$$

تعريف $\overline{\varphi}$

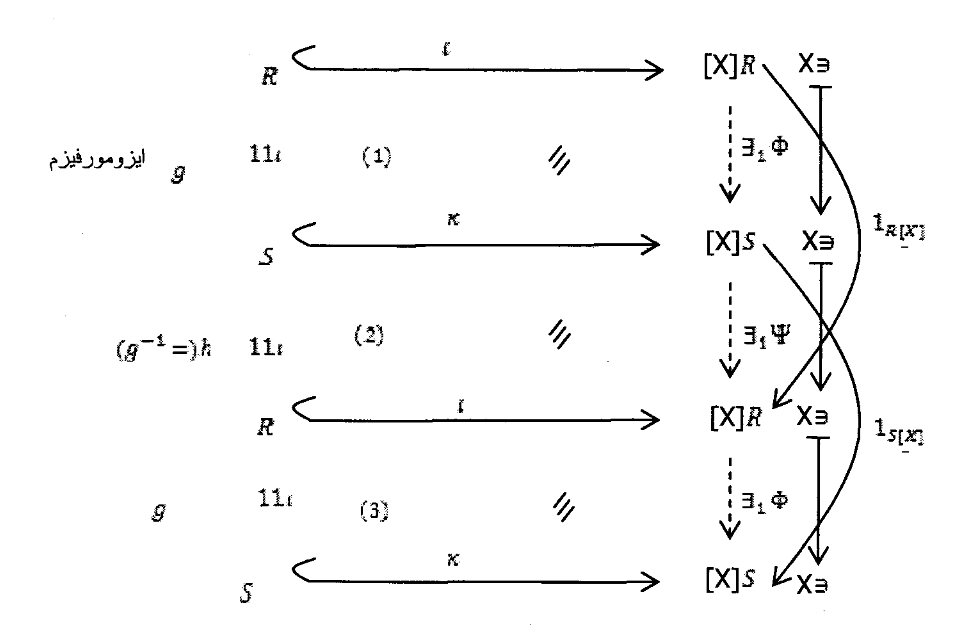
ولأن $\varphi(1_R) = 1_S$ يكون (3) $\overline{\varphi}(1_{R[X]}) = 1_{S[X]}$ (لأن $1_{R[X]} = 1_R$ ، $1_{S[X]} = 1_S$)

من (1) ، (2) ، (3) $\overline{\varphi}$ هومومورفيزم .

<u>مثال ٣٠ :</u>

برهن على أنه إذا كانت R ، S حلقتين متشاكلتين ، فإن $R[X]$ ، $S[X]$ متشاكلتان .

<u>البرهان</u> : سنستخدم المسألة الكونية (العالمية) لكثيرات الحدود



فى الشكل (١) $R[X]$ هو حل المسألة الكونية ، ويوجد هومومورفيزم وحيد Φ يجعل الشكل إبدالياً . ويرسم X فى X .

فى الشكل (2) $S[X]$ هو حل المسألة الكونية ، ويوجد هومومورفيزم وحيد Ψ يجعل الشكل إبدالياً . ويرسم X فى X .

فى الشكل (3) $R[X]$ هو حل المسألة الكونية ، ويوجد هومومورفيزم وحيد لابد أن يكون هو Φ بحيث يجعل الشكل إبدالياً . ويرسم X فى X .

ولكن الهومومورفيزمين $1_{R[X]}$ ، $1_{S[X]}$ يجعلان الشكل المكون من (1) ، (2) والشكل المكون من (2) ، (3) على الترتيب إبداليين . ومن حيث أن Φ ، Ψ تفعلان نفس الشيء وهما وحيدتان فينتج أن : $\psi\Phi = 1_{R[X]}(3)$ ، $\Phi\psi = 1_{S[X]}(4)$

من (3) يكون Φ راسماً واحداً لواحد ، و ψ راسماً شاملاً (غامراً)

ومن (4) يكون ψ راسماً واحداً لواحد ، Φ راسماً شاملاً (غامراً)

Φ هومومورفيزم (كذلك ψ) فيكون Φ (كذلك ψ) أيزومورفيزم .

نهاية البرهان .

<u>مثال ٣١</u> : بإضافة الفرض الآتى فى تعريف النطاق الإقليدى (R, d) :

$$\forall a,b \in \mathbb{R} \setminus \{0\} : d(a) \leq d(ab)$$

برهن على أن $d(1)$ هو الأصغر لجميع $a \in R \setminus \{0\}$. برهن كذلك على أن $u \in R$ وحدة إذا كان وفقط إذا كان $d(u) = 1$.

<u>البرهان</u> : لجميع $a \in R \setminus \{0\}$ لدينا :

$$d(1) \leq d(1a) = d(a) \qquad (1)$$

والآن بفرض أن لدينا $u \in R$ وحدة :

$$d(u) \leq d(uu^{-1}) = d(1) \qquad (2)$$

من (1) ، (2) ينتج أن $d(u) = 1$

وبالعكس إذا كان $u \in R$ بحيث إن $d(u) = d(1)$. فبخوارزمية القسمة يوجد $g, r \in R$ بحيث إن :

$$1 = qu + r, \quad r = 0 \text{ أو } d(r) < d(u)$$

ولكن $d(u) = d(1)$ هو الأصغر بين $d(x)$ لجميع $x \in R \setminus \{0\}$ ، فإن $d(r) < d(u)$ يكون مستحيلا ويلزم أن يكون $r = 0$. أى أن : $1 = q\,u$ وتكون u وحدة .

<u>مثال ٣٢</u> : مع اعتماد الفرض المضاف فى مثال ٣١ السابق مباشرة حدد إذا ما كانت التقريرات الآتية صحيحة أم خاطئة حيث (R, d) نطاق إقليدى :

(أ) $\forall a \in R \setminus \{0\} : d(1) \le d(a)$

(ب) $\forall a \in R \setminus \{0,1\} : d(1) < d(a)$

(جـ) $d(1) < d(a)$: (ليس وحدة) $\forall a \in R \setminus \{0\}, a \notin R^*$

<u>الحل</u> :

(أ) صحيحة

(ب) خاطئة لأن فى حالة كون $a \in R^*$ أى وحدة فإن $d(1) = d(a)$

(جـ) صحيحة

<u>مثال ٣٣</u> : حقق نتائج مثال ٣١ فى حالة كون النطاق الإقليدى هو $(\mathbb{Z}[i], d)$ حيث

$$d : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$$
$$m + in \mapsto m^2 + n^2$$

(مثال ٣ فى (٢-١-٨))

<u>الحل</u> : سنبرهن فى مثال ٣ من (٣-٢-١١) على أن وحدات $\mathbb{Z}[i]$ هى فقط ± 1 ، $\pm i$.

$$d(1) = d(i) = 1^2 = 1, d(-1) = d(-i) = (-1)^2 = 1$$

وواضح أن $d(1)$ هو الأصغر بين جميع $d(m + in)$ حيث $0 \ne m + in \in \mathbb{Z}[i]$.

<u>مثال ٣٤</u> : حدد إذا ما كانت التقارير الآتية صحيحة أم خاطئة :

(أ) إذا كان F حقلاً جزئياً من حقل E ، وكان $a \in E$ صفراً لكثيرة الحدود $f(X) \in F[X]$ ، فإن a سيكون صفراً لكثيرة الحدود $h(X) := f(X)g(X)$ لجميع $g(X) \in F[X]$

(ب) إذا كان F حقلاً جزئياً من حقل E ، وكان $f(X) \in F[X]$ ، عندئذ فإن مجموعة أصفار $f(X)$ فى E تكون مثالياً فى E .

(جـ) إذا كان F حقلاً جزئياً من حقل E ، وكان $\alpha \in E$ ، عندئذ فإن مجموعة جميع $f(X) \in F[X]$ بحيث إن $f(\alpha) = 0$ تكون مثالياً فى $F[X]$

<u>تعريف الحقل الجزئى</u> : ليكن K حقلاً . يقال إن $k \subset K$ حقل جزئى (subfield) من K إذا كان وفقط إذا كان :

(أ) $\forall a,b \in k : a+b \in k , ab \in k$

(ب) k مع العمليتين المستحدثتين

$$+ : k \times k \to k \quad , \quad . : k \times k \to k$$
$$(a,b) \mapsto a+b \quad , \quad (a,b) \mapsto a.b$$

يكون حقلاً .

<u>الحـل</u> : (أ) $h(a) = f(a)g(a) = 0g(a) = 0$ ، أى صحيحة

(ب) ليكن $\mathbb{R}[X] \ni f := X^2 + 1$. f لها جذران فى $\mathbb{C}[X]$ هما $\pm i$ لكن $i-(-i) = 2i$ ليس جذراً لـــ f . إذن التقرير خاطئ .

(جـ) صحيحة لأنه أولاً هذه المجموعة غير خالية، فهى تحتوى على الأقل كثيرة الحدود "0" .

وإذا كان هناك $f, g \in F[X]$ بحيث إن $f(\alpha) = g(\alpha) = 0$ فإن :

$(f-g)(\alpha) = f(\alpha) - g(\alpha) = 0$. وإذا كان $f \in F[X]$ بحيث إن $f(\alpha) = 0$ ، وكان $h \in F[X]$ فإن $fh(\alpha) := f(\alpha)h(\alpha) = 0h(\alpha) = 0$. إذن التقرير صحيح (تذكر أن $F[X]$ حلقة إبدالية) .

مثال ٣٥ : حدد إذا ما كانت التقارير الآتية ، صائبة أم خاطئة :

(أ) كثيرة الحدود f من درجة n ذات معاملات من حقل F يكون لها على الأكثر n من الأصفار فى F .

(ب) كثيرة الحدود f من درجة n ذات معاملات من حقل F يكون لها على الأكثر n من الأصفار فى أى حقل E بحيث يكون $F \subset E$.

(جـ) كل مثالى فى $F[X]$ حيث F حقل يكون مثالياً أساسياً .

(د) كل مثالى أساسى فى $F[X]$ حيث F حقل يكون مثالياً أعظم .

الحل : (أ) ، (ب) ، (جـ) صائبة . (د) خاطئ .

مثال ٣٦ : بدون استخدام النظرية (٢-١-١٠) برهن على أن $\mathbb{Z}[X]$ ليس نطاق مثاليات أساسية .

البرهان : لنأخذ مثالياً اختيارياً I فى $\mathbb{Z}[X]$ معرفاً كالآتى :

$$I := \{aX + 2b) \mid a,b \in \mathbb{Z}\}$$

ولنفترض أن I يمكن كتابته على الصورة $I = [h(X)]$ ، أى هو مثالى أساسى . عندئذ فإنه توجد كثيرتا حدود $f(X)$ ، $g(X)$ فى $\mathbb{Z}[X]$ بحيث إن : $2 = h(X)f(X)$ ، $X = h(X)g(X)$ ، لأن $2, X \in I$. ومن (٢-١-٥) يكون $1 = \deg(h(X)) + \deg(g(X))$ ، $0 = \deg(h(X)) + \deg(f(X))$ (تذكر أن $\mathbb{Z}[X]$ نطاق متكامل) وينتج مباشرة أن $f(X)$ ، $h(X)$ ثابتتان .

كذلك فإن $f(X) = \pm 1$ ، $h(X) = \pm 2$ أو $f(X) = \pm 2$ ، $h(X) = \pm 1$. ولكن $h(X) \neq \pm 1$ وإلا كان $[h(X)] = \mathbb{Z}[X]$. ومن ثم فإن $h(X) = \pm 2$ وبالتالى فإن $g(X) = \pm \frac{1}{2} X$ وهذا تناقض لأن $g(X) \in \mathbb{Z}[X]$. أى أن I لايمكن أن يكون مثالياً أساسياً . وبالتالى فإن $\mathbb{Z}[X]$ ليس نطاق مثاليات .

تمارين

(١) اقسم فى $\mathbb{Z}_5[X]$ كثيرة الحدود $f := X^4 - \bar{3}X^3 + \bar{2}X^2 + \bar{4}X - \bar{1}$ على كثيرة الحدود $g := X^2 - \bar{2}X + \bar{3}$

(٢) اقسم فى $\mathbb{Z}_5[X]$ كثيرة الحدود $X^4 + \bar{3}X^3 + \bar{2}X + \bar{4}$ على كثيرة الحدود $X - \bar{1}$.

(٣) ليكن $f := X^6 + \bar{3}X^5 + \bar{4}X^2 - \bar{3}X + \bar{2} \in \mathbb{Z}_7[X]$ ، $g := X^2 + \bar{2}X - \bar{3}$ ، اوجد $q, r \in \mathbb{Z}_7[X]$ بحيث يكون $f = qg + r$ ، $\deg(r) < 2$

(٤) ليكن $f := X^6 + \bar{3}X^5 + \bar{4}X^2 - \bar{3}X + \bar{2} \in \mathbb{Z}_7[X]$ ، $g := \bar{3}X^2 + \bar{2}X - \bar{3}$ ، اوجد $q, r \in \mathbb{Z}_7[X]$ بحيث يكون $f = qg + r$ ، $\deg(r) < 2$

(٥) برهن على أن $X^4 + X \in \mathbb{Z}_3[X]$ ، $X^2 + X$ تعينان نفس الدالة من $\mathbb{Z}_3$ إلى $\mathbb{Z}_3$

(٦) هل هناك أى كثيرات حدود غير ثابتة فى $\mathbb{Z}[X]$ يكون لها معكوس ضربى ؟ فسر إجابتك

(٧) ليكن p عدداً أولياً . هل هناك أية كثيرات حدود غير ثابتة فى $\mathbb{Z}_p[X]$ لها معكوس ضربى .

(إرشاد : انظر (٢-١-٥ (٢)))

(٨) برهن على أن المثالى $[X]$ يكون مثالياً أعظم فى $\mathbb{Q}[X]$

(٩) ليكن F حقلاً غير منته ، $f(X), g(X) \in F[X]$. إذا كان $f(a) = g(a)$ لعدد غير منته من العناصر a فى F . برهن على أن $f(X) = g(X)$

(١٠) ليكن F حقلاً ، ولتكن $p(X) \in F[X]$. إذا كانت $f(X), g(X) \in F[X]$ ، وكانت $\deg(f(X)), \deg(g(X)) < \deg(p(X))$ ، فبرهن على أن : $f(X) + [p(X)] = g(X) + [p(X)]$ يستلزم أن $f(X) = g(X)$

(١١) لتكن $f(X) \in \mathbb{R}[X]$. ليكن $f(a) = 0$ ، لكن $f'(a) \neq 0$ ، حيث $f'(X)$ مشتقة الدالة $f(X)$. برهن على أن a صفر غير مكرر لكثيرة الحدود $f(X)$

(١٢) اضرب مثالاً لبيان أن التمهيدية (٢-٢-٢) تكون خاطئة إذا استبدلنا $\mathbb{Z}_m$ حيث m ليس عدداً أولياً ، $m > 1$ بـ R النطاق المتكامل .

(١٣) ليكن F حقلاً ، وليكن

$$I := \{a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \mid a_n, a_{n-1}, \ldots, a_0 \in F, a_n + a_{n-1} + \ldots + a_0 = 0\}$$

برهن على أن I مثالى فى $F[X]$ ، واوجد مولداً (generator) لـ I .

(١٤) اوجد عدداً غير منته من كثيرات الحدود $f(X)$ فى $\mathbb{Z}_3[X]$ بحيث يكون $f(a) = \overline{0}$ لجميع $a \in \mathbb{Z}_3$.

(١٥) برهن أو انف : D نطاق مثاليات أساسية $\Leftarrow D[X]$ نطاق مثاليات أساسية .

(١٦) برهن أو انف : أى نطاق جزئى من نطاق إقليدى يكون نطاقاً إقليدياً .

2 Ring Theory نظرية الحلقات

القسم

الباب

3

القسمة فى النطاق المتكامل

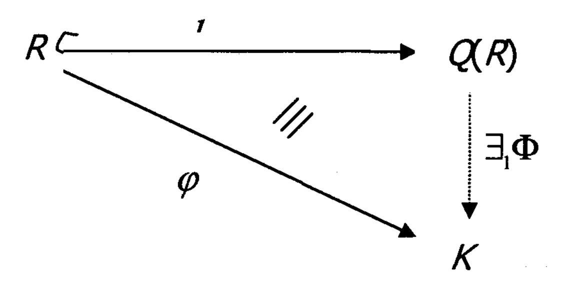
Division in Integral Domains

٣-١ حقل القسمة لنطاق متكامل Quotient filed of an integral domain

٣-١-١ تعريف :

ليكن R نطاقاً متكاملاً . يقال للزوج $(Q(R),\iota)$ المكون من حقل $Q(R)$ ، ومونومورفيزم حلق $\iota : R \to Q(R)$ إنه **حقل القسمة** (Quotient field) لـ R إذا تحققت الخاصة الكونية (العالمية) :

لكل حقل K ، ولكل مونومورفيزم حلق $\varphi : R \to K$ ، يوجد بالضبط مونومورفيزم حلق وحيد $\Phi : Q(R) \to K$ بحيث إن الشكل الآتى يكون إبداليا:



٣-١-٢ نظرية :

ليكن R نطاقاً متكاملاً . (١) بواسطة :

$$(a,b) \sim (c,d) :\Leftrightarrow ad = bc$$

ستعرف علاقة تكافؤ على $R \times (R \setminus \{0\})$

(٢) سنشير بـ $\frac{a}{b}$ إلى فصل التكافؤ لـ $(a,b) \in R \times (R \setminus \{0\})$ ، بـ $Q(R)$ إلى مجموعة كل فصول التكافؤ هذه ، وهكذا يوجد رابطان "+" ، "." على $Q(R)$ بحيث إن :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \frac{a}{b} . \frac{c}{d} = \frac{ac}{bd} \qquad \forall a,c \in R \;\; \forall b,d \in R \setminus \{0\}$$

(٣) الثلاثى $(Q(R),+,.)$ حقل

(٤) الراسم : $\begin{array}{l} \iota : R \to Q(R) \\ a \mapsto \dfrac{a}{1} \end{array}$ هو مونومورفيزم حلق

(٥) الزوج $(Q(R),\iota)$ هو حقل القسمة لـــ R

<u>البرهان</u> :

(١)

$$\forall a,b\in R\times(R\setminus\{0\}):ab=ba\Rightarrow\ \ \forall(a,b)\in R\times(R\setminus\{0\}):(a,b)\sim(a,b)$$

أى أن "~" انعكاسية (reflexive)

$$\forall(a,b),(c,d)\in R\times R\setminus\{0\}:(a,c)\sim(c,d)\Rightarrow$$

$$ad=bc\Rightarrow cb=da\Rightarrow(c,d)\sim(a,b)$$

أى أن "~" متماثلة

$$\forall(a,b),(c,d),(e,f)\in R\times(R\setminus\{0\}):(a,b)\sim(c,d),(c,d)\sim(e,f)\Rightarrow$$

$$ad=bc,cf=de\Rightarrow(ad)f=(bc)f,b(cf)=b(de)\Rightarrow(ad)f=b(de)$$

$$\Rightarrow\quad af=be\Rightarrow(a,b)\sim(e,f)$$

نطاق متكامل $R,$

$d\neq 0$

أى أن "~" انتقالية (transitive) ، ومن ثم فإنها علاقة تكافؤ .

(٢) نبرهن على أن الرابطين "+" ، "." معرفان جيداً ، أى أنه من $\dfrac{a'}{b'}=\dfrac{a}{b}$ ، $\dfrac{c'}{d'}=\dfrac{c}{d}$ ينتج أن :

$$\frac{a'd'+b'c'}{b'd'}=\frac{ad+bc}{bd},\frac{a'c'}{b'd'}=\frac{ac}{bd}:$$

لدينا :

$$\frac{a'}{b'}=\frac{a}{b},\frac{c'}{d'}=\frac{c}{d}\Rightarrow a'b=ab',c'd=cd'\Rightarrow a'bdd'=ab'dd',$$

$$c'dbb'=cd'bb'\Rightarrow(a'd'+b'c')bd=(ad+bc)b'd'\Rightarrow\frac{a'd'+b'c'}{b'd'}=\frac{ad+bc}{bd}$$

كذلك لدينا $a'bc'd=ab'cd'$ ومنها ينتج مباشرة أن : $\frac{a'c'}{b'd'}=\frac{ac}{bd}$.

(٣) يمكن للقارئ أن يتحقق بسهولة من أن $(Q(R),+,.)$ حلقة إبدالية ، عنصر الوحدة فيها هو $\frac{1}{1}$ لأن :

$$\forall\frac{a}{b}\in Q(R):\frac{a}{b}.\frac{1}{1}=\frac{a.1}{b.1}=\frac{a}{b}=\frac{1.a}{1.b}=\frac{1}{1}.\frac{a}{b}$$

(1 هو عنصر الوحدة فى R)

كذلك فإن $\frac{0}{1}$ هو عنصر الصفر فى $Q(R)$ لأن :

$$\forall\frac{a}{b}\in Q(R):\frac{0}{1}+\frac{a}{b}=\frac{0b+1a}{1b}=\frac{1a}{1b}=\frac{a}{b}$$

كذلك فإن معكوس $\frac{a}{b}$ بالنسبة للعملية "+" هو $\frac{-a}{b}$ لأن :

$$\frac{-a}{b}+\frac{a}{b}=\frac{-ab+ba}{bb}=\frac{0}{b^2}=\frac{0}{1}$$

(0 هو العنصر الصفرى فى R)

(لأن $\frac{0}{b^2}=\frac{0}{1}\Leftrightarrow 01=b^2 0$)

كذلك فإن $\frac{1}{1}\neq\frac{0}{1}$ وإلا :

$$(1)(1)=(1)(0)\Rightarrow 1=0$$

وهذا تناقض لأن R نطاق متكامل وبالتالى $1\neq 0$

لكل $\frac{a}{b} \in Q(R) \setminus \{0\}$ (أى أن $a \neq 0$) يوجد $\frac{b}{a} \in Q(R) \setminus \{0\}$ وينتج أن :

$$\frac{a}{b} . \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$$

(لأن $ab1 = ba1$)

أى أن لكل عنصر فى $Q(R) \setminus \{0\}$ يوجد معكوس بالنسبة للعملية (للرابط) "." .

أى أن $(Q(R), +, .)$ حقل .

(٤) الراسم $\begin{matrix} \iota : R \to Q(R) \\ a \mapsto \frac{a}{1} \end{matrix}$ مونومورفيزم لأن :

$$\forall a, b \in R : \iota(a) = \iota(b) \Rightarrow \frac{a}{1} = \frac{b}{1} \Rightarrow a1 = 1b \Rightarrow a = b$$

أى أن ι راسم واحد لواحد (أحادى)

$$\iota(a+b) = \frac{a+b}{1} = \frac{a1 + 1b}{(1)(1)} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b)$$

$$\iota(ab) = \frac{ab}{1} = \frac{ab}{(1)(1)} = \frac{a}{1} . \frac{b}{1} = \iota(a) . \iota(b)$$

$$\iota(1) = \frac{1}{1}$$

أى أن ι هومومورفيزم وبالتالى هو مونومورفيزم

يتبقى أن نثبت أن الخاصة العالمية (الكونية) متحققة :

(٥) ليكن K حقلاً ، $\varphi : R \to K$ مونومورفيزماً حلقياً . إذا كان $\Phi : Q(R) \to K$ مونومورفيزماً حلقياً بحيث إن $\Phi o \iota = \varphi$ فإن :

$$\forall \frac{a}{b} \in Q(R) : \Phi(\frac{a}{b}) = \Phi(\frac{a1}{1b}) = \Phi(\frac{a}{1} . \frac{1}{b}) = \Phi(\iota(a) . \iota(b)^{-1})$$

$$= \Phi(\iota(a))\Phi(\iota(b))^{-1} = \varphi(a)\varphi(b)^{-1}$$

أى أنه يوجد على الأكثر Φ واحدة تحقق المطلوب .

ونثبت الآن أنه يوجد بالفعل هذه لـــ Φ كالآتى :

ليكن $\Phi : Q(R) \to K$ بحيث إن $\Phi(\frac{a}{b}) = \varphi(a)\varphi(b)^{-1}$ لجميع $\frac{a}{b} \in Q(R)$

وليكن $\frac{a'}{b'} = \frac{a}{b}$. عندئذ فإنه ينتج أن : $a'b = ab'$ وبالتالى فإن :

$$a'b = ab' \Rightarrow \varphi(a')\varphi(b) = \varphi(a)\varphi(b') \Rightarrow \varphi(a)\varphi(b)^{-1} = \varphi(a')\varphi(b')^{-1}$$

أى أن $\Phi(\frac{a}{b}) = \Phi(\frac{a'}{b'})$ أى أن Φ معرفة جيداً (موجودة)

ونبرهن أخيراً على أن الراسم ϕ هومومورفيزم بالفعل كالآتى :

$$\forall \frac{a}{b}, \frac{c}{d} \in Q(R) : \Phi(\frac{a}{b} + \frac{c}{d}) = \Phi(\frac{ad+bc}{bd}) = \varphi(ad+bc)\varphi(bd)^{-1}$$

$$= \varphi(ad+bc)(\varphi(b)\varphi(d))^{-1} = (\varphi(a)\varphi(d) + \varphi(b)\varphi(c))\varphi(d)^{-1}\varphi(b)^{-1}$$

$$= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} = \Phi(\frac{a}{b}) + \Phi(\frac{c}{d}),$$

$$\Phi(\frac{a}{b}.\frac{c}{d}) = \Phi(\frac{ac}{bd}) = \varphi(ac)\varphi(bd)^{-1} = \varphi(a)\varphi(c)(\varphi(b)\varphi(d))^{-1}$$

$$= \underset{K \text{ إبدالى}}{\varphi(a)\varphi(c)\varphi(b)^{-1}\varphi(d)^{-1}} = \underset{K \text{ إبدالى}}{\varphi(a)\varphi(b)^{-1}\varphi(c)\varphi(d)^{-1}} = \Phi(\frac{a}{b})\Phi(\frac{c}{d}),$$

$$\Phi(\frac{1}{1}) = \varphi(1)\varphi(1)^{-1} = 1$$

أى أن Φ هومومورفيزم .

نهاية البرهان .

٣-١-٣ ملحوظة :

لاحظ أن حقل القسمة لنطاق متكامل هو أصغر حقل يحتوى على النطاق المتكامل . ويقال فى هذه الحالة إن النطاق المتكامل قد غمر (embedded) فى الحقل . (انظر مثال ٤٠ فى (١-٢-٨)) . فإذا كان K هو حقل القسمة لـ R النطاق المتكامل ، وكان $\bar{K}$ حقلاً آخر يحتوى على R فإن : $R \subset K \subset \bar{K}$

٣-١-٤ أمثلة :

(١) $\mathbb{Z}$ نطاق متكامل ، حقل القسمة لـ $\mathbb{Z}$ هو $\mathbb{Q}$:

$$\mathbb{Z} \underset{\neq}{\subseteq} \mathbb{Q} \underset{\neq}{\subseteq} \mathbb{R} \underset{\neq}{\subseteq} \mathbb{C}$$

(٢) حقل القسمة لنطاق متكامل منته (finite integral domain) هو نفسه ، لأن النطاق المتكامل المنتهى يكون حقلاً ، وهو بالطبع أصغر حقل يحتوى على نفسه .

(٣) ليكن K حقلاً . ينتج أن $K[X]$ نطاق متكامل . يشار إلى حقل القسمة لـ $K[X]$ بالرمز $K(X)$ غالباً ، ويسمى حقل الدوال الكسرية أو حقل الدوال النسبية (The field of relational functions) فى غير المحدد X ، والمعاملات من K .

(٤) الحقل $M(\mathbb{C})$ حقل الدوال الميرومورفية (The field of meromorphic functions) على $\mathbb{C}$ هو حقل القسمة لـ $H(\mathbb{C})$ النطاق المتكامل للدوال الهولومورفية (التحليلية ، القابلة للتفاضل) على $\mathbb{C}$.

٣-١-٥ أمثلة محلولة :

__مثال ١__ : صف حقل القسمة للنطاق المتكامل الجزئى(The integral subdomain) الآتى:

$$D := \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$$

__الحل__: حقل القسمة لـ D هو أصغر حقل يحتوى D ، الذى يكون فيه المعكوس الضربى لكل عنصر فى $D \setminus \{0\}$ ، أى يكون هو :

$$\{\frac{m - n\sqrt{2}}{m^2 + 2n^2} \mid m, n \in \mathbb{Z}, m^2 + 2n^2 \neq 0\} = \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$$

مثال٢ : حدد إذا ما كانت التقارير الآتية صحيحة أم خاطئة :

(أ) $\mathbb{R}$ هو حقل القسمة لـ $\mathbb{R}$

(ب) $\mathbb{C}$ هو حقل القسمة لـ $\mathbb{R}$

(جـ) إذا كان D حقلاً فإن حقل قسمة لـ D يكون متشاكلاً (أيزومورفيزماً) مع D .

(د) حقيقة أن النطاق المتكامل R ليس له قواسم صفرية قد استخدمت بقوة عدة مرات فى إنشاء حقل القسمة $\mathbb{Q}(R)$

(هـ) كل عنصر فى النطاق المتكامل R ، يكون وحدة فى حقل القسمة $\mathbb{Q}(R)$

(و) كل عنصرغير صفرى فى النطاق المتكامل R، يكون وحدة فى حقل القسمة $\mathbb{Q}(R)$

(ز) حقل القسمة F' لنطاق متكامل جزئى D' من نطاق متكامل D يمكن اعتباره حقلاً جزئياً من حقل قسمة لـ D .

الحل : (أ) ، (جـ) ، (د) ، (و) ، (ز) صحيحة ، (ب) ، (هـ) خاطئتان .

مثال ٣ : برهن على أن حقل القسمة للنطاق المتكامل

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$$

يكون

$$\mathbb{Q}[i] := \{r + si \mid r, s \in \mathbb{Q}\}$$

البرهان : أى حقل يحتوى على $\mathbb{Z}$ ، يجب أن يحتوى على $\mathbb{Q}[i]$. (*)

والآن ليكن $a+bi, c+di \in \mathbb{Z}[i]$ ، $c+di \neq 0$:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd+i(bc-ad)}{c^2+d^2} \in \mathbb{Q}[i]$$

أى أن حقل القسمة لـ $\mathbb{Z}[i]$ هو حقل محتوى فى $\mathbb{Q}[i]$. ومع (*) ينتج المطلوب مباشرة .

تمارين

(١) لتكن R حلقة إبدالية ، ولتكن $T \neq \{0\}$ مجموعة غير خالية من R ، مغلقة بالنسبة إلى الضرب (closed under multiplication) ولاتحتوى قواسم صفرية .

مبتدئاً بـــ $R\times T$ يمكنك أن تكبر R إلى حلقة قسمة جزئية $Q(R, T)$ متبعاً نفس الأسلوب تقريباً فى إنشاء حقل القسمة لنطاق متكامل . برهن على وجه الخصوص أن :

(أ) $Q(R, T)$ لها عنصر وحدة حتى إذا لم يكن لـــ R عنصر وحدة .

(ب) فى $Q(R, T)$ كل عنصر غير صفرى من T يكون وحدة

(٢) بالاشارة إلى التمرين (١) ، كم عدد عناصر الحلقة $Q(\mathbb{Z}_4,\{\bar{1},\bar{3}\})$ ؟

(إرشاد : $\bar{1}$ ، $\bar{3}$ وحدتان فى $\mathbb{Z}_4$. عدد العناصر المطلوب 4) .

(٣) بالإشارة إلى التمرين (١) صف الحلقة $Q(\mathbb{Z},\{2^n \mid n\in \mathbb{N}\})$ ، وذلك بوصف حلقة جزئية من $\mathbb{R}$ تكون متشاكلة معها .

(الحلقة الجزئية المطلوبة هى $\{\frac{m}{2^n} \mid m\in \mathbb{Z}, n\in \mathbb{N}\}$)

(٤) بالإشارة كذلك إلى التمرين (١) صف الحلقة $Q(3\mathbb{Z},\{6^n \mid n\in \mathbb{N}\})$ بوصف حلقة جزئية من $\mathbb{R}$ تكون متشاكلة معها .

(٥) حدد إذا ما كان التقريران الآتيان صحيحين أم خاطئين .

(أ) إذا كان F حقلاً فإن وحدات $F[X]$ هى بالضبط العناصر غير الصفرية فى F .

(ب) إذا كان F حقلاً ، فإن وحدات $F(X)$ (= حقل القسمة لـــ $F[X]$) هى بالضبط العناصر غير الصفرية فى F .

(٦) برهن على أن حقل القسمة لحقل F يكون متشاكلا مع F .

(٧) وضح لماذا لايمكن أن ننشئ حقل القسمة لحلقة إبدالية ذات عنصر وحدة ، لكنها ليست نطاقاً متكاملاً .

(٨) ليكن D نطاقاً متكاملا ، وليكن F حقل القسمة لـــ D . برهن على أنه إذا كان E أى حقل يحتوى D ، فإن E يحتوى حقلاً يتشاكل مع F . (أى أن حقل القسمة لنطاق متكامل D يكون أصغر حقل يحتوى على D) .

٣-٢ العناصر الأولية والعناصر غير القابلة للتبسيط

Prime elements and irreducible elements

٣-٢-١ تعريف :

ليكن a،b عنصرين فى نطاق متكامل R. يسمى b قاسما(divisor) لــa ، إذا وجد $c\in R$ بحيث إن: $a=bc$. ونكتب (كما سبق) $b|a$ ، بينما نكتب $b\nmid a$ إذا لم يكن الأمر كذلك.

ونسطيع بسهولة شديدة البرهنة على الملحوظة الآتية :

٣-٢-٢ ملحوظة :

ليكن R نطاقا متكاملا ، $1\in R$ عنصر الوحدة فيه . عندئذ فإن :

(أ) لجميع $a\in R$: $1|a$ ، $a|a$

(ب) $c|b$ ، $b|a$ $\Leftarrow$ $c|a$

(جـ) لجميع $x_1,x_2,...,x_n\in R$: $b|a_1$ ، $b|a_2$ ،... ، $b|a_n$ $\Leftarrow$ $b|(x_1a_1+x_2a_2+...+x_na_n)$

(د) $b|1 \Leftrightarrow b\in R^*$ ($R^*=R\setminus\{0\}$ ، كما سبق)

(هـ) لجميع $u\in R^*$: $b|a$ $\Leftarrow$ $(bu)|a$

(و) $[a]\subset[b] \Leftrightarrow b|a$ ($[a]$ المثالى المتولد من a ، كما سبق)

٣-٢-٣ : تعريف :

ليكن R نطاقا متكاملا . يقال لعنصرين $a,b\in R$ إنهما يتشاركان أو متشاركان (associate) إذا وجد $u\in R^*$ بحيث إن $a=bu$. ونكتب فى هذه الحالة $a\sim b$ ، وإذا لم يكن الأمر كذلك نكتب $a\nsim b$.

٣-٢-٤ ملحوظة :

ليكن R نطاقا متكاملا .

(أ) لجميع $a,b\in R$: $[a]=[b] \Leftrightarrow a\sim b$

(ب) $a,b\in R^*$: $a\sim b \Leftrightarrow [b|a$ ، $a|b]$

(جـ) $\sim$ علاقة تكافؤ على R .

<u>البرهان</u> :

(أ) "$\Leftarrow$" : $[a]=[b]$ $\Leftarrow$ يوجد $u,v\in R$: $a = bu$ ، $b = av$ $\Leftarrow$ يوجد

$u,v\in R$: $a = a\,v\,u$ $\Leftarrow$ $u\,v = 1$

R نطاق متكامل

أى أن $u,v\in R^*$ $\Leftarrow$ $a \sim b$

"$\Rightarrow$" : $a \sim b$ $\Leftarrow$ يوجد $u\in R^*$: $a = bu$ $\Leftarrow a\in [b]$

$\Leftarrow$ $[a]\subset[b]$. بالمثل $[b]\subset[a]$ ، وينتج أن : $[a]=[b]$

(ب) "$\Leftarrow$" : $a \sim b$ $\Leftarrow$ يوجد $c\in R^*$: $a = b\,c$ $\Leftarrow$ $b\,|\,a$.

$c\in R^*$ $\Leftarrow$ يوجد $d\in R^*$: $c\,d = 1 \Leftarrow b\,c\,d = b = a\,d$ $\Leftarrow a\,|\,b$.

"$\Rightarrow$" : $a\,|\,b$ ، $b\,|\,a \Leftarrow$ يوجد $c,d\in R$: $a\,c = b$ ، $b\,d = a$ $\Leftarrow$ يوجد

$c,d\in R$: $b\,d\,c = b$ $\Leftarrow$ $d\,c = 1$ أى أن $c,d\in R^*$ $\Leftarrow$ $a \sim b$

R نطاق متكامل

(جـ) لجميع $a\in R$: $a = 1\,a$ أى أن لجميع $a\in R$: $a \sim a$. أى أن ~ انعكاسية .

لجميع $a,b\in R$: $a \sim b$ $\Leftarrow$ يوجد $c\in R^*$: $a = b\,c$ ، يوجد $d\in R^*$: $c\,d = 1$

$\Leftarrow$ يوجد $c,d\in R^*$: $b = b\,c\,d = a\,d$ أى أن $b \sim a$.

أى أن ~ متماثلة .

لجميع $a,b,c\in R$: $a \sim b$ ، $b \sim c$ $\Leftarrow$ يوجد $u,v\in R^*$: $a = b\,u$ ، $b = c\,v$

$\Leftarrow$ يوجد $u,v\in R^*$: $a = c\,v\,u$. R^* زمرة بالنسبة للضرب يقتضى أن

$vu = w\in R^*$ أى أن $a = cw$ ، $w\in R^*$ وبالتالى فإن $a \sim c$.

إذن ~ انتقالية ومن ثم فهى علاقة تكافؤ .

<u>٣-٢-٥ تعريف</u> :

ليكن R نطاقاً متكاملاً .

(أ) يقال لعنصر $p \in R$ إنه **عنصر أولى** (prime element) إذا كان :

(١) $p \neq 0$ ، $p \notin R^*$

(٢) لجميع $a,b \in R$: $p \mid a\,b \Rightarrow p \mid a$ أو $p \mid b$

(ب) يقال لعنصر $q \in R$ إنه **عنصر غير قابل للتبسيط** (irreducible element) إذا كان :

(١) $q \neq 0$ ، $q \notin R^*$

(٢) لجميع $a,b \in R$: $q = a\,b \Rightarrow a \in R^*$ أو $b \in R^*$

(جـ) يقال لعنصر فى R إنه **قابل للتبسيط** (reducible) إذا لم يكن غير قابل للتبسيط .

٣-٢-٦ أمثلة :

(١) لأى حقل K : $K^* = K \setminus \{0\}$ ، وبالتالى فإن K لايحتوى على أية عناصر أولية أو عناصر قابلة للتبسيط .

(٢) لجميع $m \in \mathbb{N}, m > 1$:

m عنصر أولى فى $\mathbb{Z}$ $\Leftrightarrow m$ عدد أولى فى $\mathbb{Z}$ $\Leftrightarrow m$ غير قابل للتبسيط فى $\mathbb{Z}$.

(٣) ليكن K حقلاً ، $a \in K \setminus \{0\}$ ، $b \in K$. كثيرة الحدود $a\,X + b$ عنصر غير قابل للتبسيط فى حلقة كثيرات الحدود $K[X]$ لأن :

$a\,X + b = f\,g$ حيث $f, g \in K[X]$ $\Rightarrow \deg(f) = 0$ أو $\deg(g) = 0$ $\Rightarrow$

$f \in K^* (= (K[X])^*)$ أو $g \in K^*$ (انظر (٢-١-٥ (٢) ، (٤)))

(٤) تطبيقاً على (٣) : كثيرة الحدود $2(X+1)$ غير قابلة للتبسيط فى $\mathbb{R}[X]$ (لأن $2 \in \mathbb{R}^*$) بينما هى قابلة للتبسيط فى $\mathbb{Z}[X]$ (لأن $\mathbb{Z}^* = \{-1, 1\}$ ، $2 \notin \mathbb{Z}^*$ ، $X+1 \notin \mathbb{Z}^*$)

٣-٢-٧ نظرية :

ليكن R نطاقاً متكاملاً ، $p \in R$

(١) p غير قابل للتبسيط $\Leftarrow p$ عنصر أولى

(٢) مثالى أولى $[p]$ ، $[p] \neq \{0\} \Leftrightarrow p$ عنصر أولى

(٣) $\nexists a \in R : [p] \subsetneq [a] \subsetneq R \Leftrightarrow p$ عنصر غير قابل للتبسيط .

البرهان :

(١) ليكن $a,b\in R$: $p=a\,b$. p عنصر أولى يستلزم أن $p\mid a$ أو $p\mid b$. $p\mid a$ يقتضى أنه يوجد $c\in R$: $a=p\,c$ ومن ثم فإن $p=a\,b=p\,c\,b$. R نطاق متكامل يقتضى أن : $1=c\,b$ أى أن $b\in R^*$. الحالة $p\mid b$ مشابهة تماماً وينتج أن $a\in R^*$.
أى أنه ينتج على أية حال أن p غير قابل للتبسيط .

(٢) "$\Rightarrow$" : p عنصر أولى $\Leftarrow$ $p\neq 0$ $\Leftarrow$ $[p]\neq\{0\}$. كذلك p عنصر أولى $\Leftarrow$ $p\notin R^*$ $\Leftarrow$ $[p]\neq R$ (لماذا ؟)

لجميع $a,b\in R$: $ab\in[p]$ $\Leftarrow$ يوجد $c\in R$: $a\,b=c\,p$ أى أن
$p\mid a\,b$ $\Leftarrow$ $p\mid a$ أو $p\mid b$ $\Leftarrow$ يوجد $d\in R$: $p\,d=a$ أو يوجد $e\in R$:
p عنصر أولى
$p\,e=b$ أى أنه $a\in[p]$ أو $b\in[p]$.

"$\Leftarrow$" : $[p]\neq\{0\}\Leftarrow p\neq 0$. $[p]$ مثالى أولى $\Leftarrow$ $[p]\neq R$ $\Leftarrow$ $1\notin[p]$ $\Leftarrow$ $p\notin R^*$.
$p\mid a\,b\Leftarrow$ يوجد $c\in R$: $p\,c=a\,b$ $\Leftarrow$ $ab\in[p]$ $\Leftarrow$ $a\in[p]$
$[p]$ مثالى أولى
أو $b\in[p]$ $\Leftarrow$ يوجد $d\in R$: $a=p\,d$ أو يوجد $e\in R$: $b=p\,e$
$\Leftarrow$ $p\mid a$ أو $p\mid b$.

(٣) "$\Rightarrow$" : ليكن هناك عنصر $a\in R$ بحيث إن $[p]\subsetneq[a]\subsetneq R$. هذا يقتضى أنه يوجد عنصر $c\in R$: $p=c\,a$ $\Leftarrow$ $c\in R^*$ أو $a\in R^*$
p عنصر غير قابل للتبسيط
$\Leftarrow[p]=[a]$ أو $[a]=R$ (لماذا ؟) : تناقض .

"$\Leftarrow$" : ليكن $p=a\,b$ ، حيث $a,b\in R$. هذا يستلزم أن $p\in[a]$

أى أن $[p]\subset[a]$ وهذا يستلزم $[p]=[a]$ أو $[a]=R$. $[a]=R$ يستلزم أن $1\in[a]$ أى أنه يوجد $c\in R$: $1=a\,c$ أى أن $a\in R^*$. $[p]=[a]$ يستلزم أنه يوجد $d\in R$ بحيث إن : $a=p\,d$. وهذا يستلزم أن : $p=p\,d\,b$ $\Leftarrow$

R نطاق متكامل

$d\,b=1$ أى أن $b\in R^*$.

٣-٢-٨ نتيجة :

ليكن R نطاق مثاليات أساسية . عندئذ فإن :

(١) $a\in R$ عنصر غير قابل للتبسيط $\Leftrightarrow$ $a\in R$ عنصر أولى

(٢) $\{0\}\neq A\subset R$ مثالى أعظم $\Leftrightarrow$ $\{0\}\neq A\subset R$ مثالى أولى .

البرهان : (١) بالرجوع إلى (٣-٢-٧ (١)) يكون المطلوب هو إثبات أن $a\in R$ عنصر غير قابل للتبسيط $\Leftarrow$ $a\in R$ عنصر أولى .

من (٣-٢-٧ (٣)) $a\in R$ عنصر غير قابل للتبسيط $\Leftarrow$ $\nexists a\in R$: $[p]\subsetneq[a]\subsetneq R$.

ومن حيث إن R نطاق مثاليات أساسية ، أى أن كل مثالى فيه يكون على الشكل $[x]$ حيث $x\in R$ فإنه ينتج أن $[p]$ مثالى أعظم فى R . ومن مثال ٢٨ فى (١-٣-٢٠) ينتج أن $[p]$ مثالى أولى ، $[p]\neq\{0\}$ ($\{0\}$ لايكون مثالياً أعظم فى أية حلقة) ومن (٣-٢-٧ (٢)) ينتج أن p عنصر أولى فى R .

(٢) كذلك من مثال ٢٨ فى (١-٣-٢٠) يتضح أن المطلوب هو إثبات أن : $\{0\}\neq A\subset R$ مثالى أولى $\Leftarrow$ $\{0\}\neq A\neq R$ مثالى أعظم .

والآن من حيث إن R نطاق مثاليات أساسية ، فكل مثالى $A\neq\{0\}$ يمكن أن يكتب على الصورة $a\in R$ ، $\{0\}\neq A=[a]$. ومن (٣-٢-٧ (٢)) ينتج أن a عنصر أولى ، ومن (٣-٢-٧ (١)) ينتج أن $a\in R$ عنصر غير قابل للتبسيط . ومن (٣-٢-٧ (٣)) ينتج أنه لايوجد عنصر $b\in R$ بحيث إن : $A=[a]\subsetneq[b]\subsetneq R$

ومن حيث إن R نطاق مثاليات أساسية فإن $A=[a]$ يكون مثالياً أعظم فى R .

٣-٢-٩ نتيجة :

ليكن K حقلاً . عندئذ فإن لكل مثالى A فى حلقة كثيرات الحدود $K[X]$ بحيث إن $\{0\} \neq A \subsetneq K[X]$ تكون التقريرات الآتية متكافئة :

(١) A مثالى أولى

(٢) A مثالى أعظم

(٣) توجد كثيرة حدود غير قابلة للتبسيط f بحيث إن : $f \in K[X], A = [f]$.

البرهان : من (٢-١-١٠) ينتج أن $K[X]$ نطاق مثاليات أساسية ، ومن (٣-٢-٨) ينتج أن التقريرين (١) ، (٢) متكافئان .

مرة أخرى $K[X]$ نطاق مثاليات أساسية ، فكل مثالى يمكن أن يكتب على الصورة $[g]$ حيث $g \in K[X]$. ومن (٣-٢-٧) :

$f \Leftrightarrow \nexists g \in K[X] : [f] \subsetneq [g] \subsetneq K[X]$ غير قابلة للتبسيط . ولأن $K[X]$ نطاق مثاليات أساسية فإن $[f]$ يكون مثالياً أعظم فى $K[X]$. أى أن التقريرين (٢) ، (٣) متكافئان .

٣-٢-١٠ مثال :

نعتبر الحلقة الجزئية من $\mathbb{C}$ الآتية :

$$\mathbb{Z}[\sqrt{-5}] := \{m + in\sqrt{5} \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$$

(تحقق من كونها حلقة جزئية من $\mathbb{C}$). هى على وجه الخصوص نطاق متكامل (تحقق كذلك من ذلك!) . الراسم $\begin{aligned} \mu : \mathbb{Z}[\sqrt{-5}] &\to \mathbb{N} \\ m + in\sqrt{5} &\mapsto m^2 + 5n^2 \end{aligned}$ يحقق الخاصة :

$$\forall x, y \in \mathbb{Z}[\sqrt{-5}] : \underline{\mu(xy)} = \mu((m_1 + in_1\sqrt{5})(m_2 + in_2\sqrt{5}))$$

$$= \mu(m_1m_2 - 5n_1n_2 + i(n_1m_2 + m_1n_2)\sqrt{5})$$

$$= (m_1m_2 - 5n_1n_2)^2 + 5(n_1m_2 + m_1n_2)^2$$

$$= m_1^2m_2^2 + 25n_1^2n_2^2 + 5n_1^2m_2^2 + 5m_1^2n_2^2 = (m_1^2 + 5n_1^2)(m_2^2 + 5n_2^2) = \underline{\mu(x)\mu(y)}$$

واضح أن 1 + ، 1 - وحدتان فى $\mathbb{Z}[\sqrt{-5}]$. نبرهن كذلك على أنه لاتوجد وحدات أخرى فى $\mathbb{Z}[\sqrt{-5}]$ كالآتى :

لتكن $u = m + in\sqrt{5}$ وحدة فى $\mathbb{Z}[\sqrt{-5}]$. هذا يستلزم وجود $v \in \mathbb{Z}[\sqrt{-5}]$ بحيث إن $u\,v = 1$.

والآن : $\mu(u)\mu(v) = \mu(uv) = \mu(1) = 1$

أى أن $\mu(u) \mid 1$ وبالتالى فإن $(m^2 + 5n^2) \mid 1$ ومن ثم فإن $n = 0$ ، $m^2 = 1$ أى أن $u \in \{-1,1\}$.

سنبرهن كذلك على علاقات القسمة الموضحة فى الجدول الآتى :

x	3	9	$2+i\sqrt{5}$	$2-i\sqrt{5}$	$3(2+i\sqrt{5})$
قواسم x (غير متشاركين مثنى مثنى)	1 3	1 3 $2 \pm i\sqrt{5}$ 9	1 $2+i\sqrt{5}$	1 $2-i\sqrt{5}$	1 3 $2+i\sqrt{5}$ $3(2+i\sqrt{5})$

والآن إذا كان z هو أحد العناصر 3 أو $2+i\sqrt{5}$ أو $2-i\sqrt{5}$ ، وكان $x \in \mathbb{Z}[\sqrt{-5}]$ قاسماً لـــ z فإنه يوجد $y \in \mathbb{Z}[\sqrt{-5}]$ بحيث إن : $x\,y = z$. ومنها ينتج أن : $\mu(x)\mu(y) = \mu(z) = 9$. ولأن $\mu(x) = 3$ غير ممكن (لأنه لايوجد $m,n \in \mathbb{Z}$ بحيث يكون $m^2 + 5n^2 = 3$) فإنه ينتج أن $\mu(x) = 1$ أو $\mu(y) = 1$ ومن ثم فإن $x \in \{1,-1\}$ أو $x \in \{z,-z\}$

وإذا كان $x = m + in\sqrt{5}$ قاسماً لـــ 9 أو لـــ $3(2+i\sqrt{5})$ فمن الخاصة $\mu(xy) = \mu(x)\mu(y)$ يتضح أن $\mu(x) = m^2 + 5n^2$ يكون قاسماً لـــ 81 ، ومن ثم

فإن $\mu(x)\in\{1,3,9,27,81\}$. وكما سبق فإن $\mu(y)\neq 3$ ، وكذلك بالمثل $\mu(y)\neq 27$ لجميع $y\in\mathbb{Z}[\sqrt{-5}]$. علاوة على ذلك فإن :

$$\mu(x)=1\Leftrightarrow x\in\{1,-1\}$$

$$\mu(x)=9\Leftrightarrow[(n=0,m^2=9)\quad \text{أو} \quad (n^2=1,m^2=4)]$$

$$\Leftrightarrow[x\in\{3,-3\}\quad \text{أو} \quad x\in\{2+i\sqrt{5},-(2+i\sqrt{5}),2-i\sqrt{5},-(2-i\sqrt{5})\}]$$

$$\mu(x)=81\Leftrightarrow[(n=0,m^2=81)\quad \text{أو} \quad (n^2=9,m^2=36)]$$

$$\Leftrightarrow[x\in\{9,-9\}\ \text{أو}\ x\in\{3(2+i\sqrt{5}),-3(2+i\sqrt{5}),3(2-i\sqrt{5},),-3(2-i\sqrt{5})\}]$$

ويلاحظ أن $2-i\sqrt{5}$ ليس قاسماً لـــ $3(2+i\sqrt{5})$. وإلا فإنه يوجد $k,\ell\in\mathbb{Z}$: $3(2+i\sqrt{5})=(2-i\sqrt{5})(k+i\ell\sqrt{5})$ وهذا يستلزم أن :

$2k+5\ell=6$ ، $-k+2\ell=3$ وبالتالى فإن : $9\ell=12$ وهذا تناقض ($\ell\in\mathbb{Z}$).

وواضح أن3، $2+i\sqrt{5}$ ، $2-i\sqrt{5}$ غير متشاركين مثنى مثنى وجميعها أعداد غير قابلة للتبسيط فى $\mathbb{Z}[\sqrt{-5}]$

ويلاحظ كذلك أن $9=3.3=(2+i\sqrt{5})(2-i\sqrt{5})$ ، أى أن 9 كتب على هيئة صورتين مختلفتين من عددين غير قابلين للتبسيط ، وهذا غير ممكن فى حالة كون الحلقة $\mathbb{Z}$ بدلاً من $\mathbb{Z}[\sqrt{-5}]$

وأخيراً فإن العنصر 3 غير القابل للتبسيط ليس عنصراً أولياً فى $\mathbb{Z}[\sqrt{-5}]$ لأن $3\mid(2+i\sqrt{5})(2-i\sqrt{5})$ بينما $3\nmid(2\pm i\sqrt{5})$.

٣-٢-١١ أمثلة محلولة

مثال ١ : قرر أى العناصر الآتية يكون غير قابل للتبسيط فى الحقل المتكامل الموضح :

(أ) $5 \in \mathbb{Z}$ (ب) $-17 \in \mathbb{Z}$

(جـ) $2X-3 \in \mathbb{Z}[X]$ (د) $14 \in \mathbb{Z}$

(هـ) $2X-3 \in \mathbb{Q}[X]$ (و) $2X-10 \in \mathbb{Z}[X]$

(ز) $\overline{2}X-\overline{10} \in \mathbb{Z}_{11}[X]$ (ح) $2X-10 \in \mathbb{Q}[X]$

الحل : واضح أن $5 \in \mathbb{Z}$ ، $-17 \in \mathbb{Z}$ غير قابلين للتبسيط (1- وحدة فى $\mathbb{Z}$) ، $14 = 7.2 \in \mathbb{Z}$ قابل للتبسيط ، $2X-3 \in \mathbb{Z}[X]$ غير قابل للتبسيط ، بينما $2X-10 = 2(X-5) \in \mathbb{Z}[X]$ قابل للتبسيط .

$2X-10 = 2(X-5) \in \mathbb{Q}[X]$: أخذنا 2 عاملاً مشتركا على سبيل المثال لكن جميع العناصر فى $\mathbb{Q}^*$ وحدات إذن $2X-10$ غير قابل للتبسيط فى $\mathbb{Q}[X]$. كذلك $2X-3 \in \mathbb{Q}[X]$ غير قابلة للتبسيط .

فى (ز) : $\overline{2}X-\overline{10} = \overline{2}(X-\overline{5}) \in \mathbb{Z}_{11}[X]$ ، $\overline{2}$ لها معكوس هو $\overline{6}$ فى $\mathbb{Z}_{11}$. أى أن $\overline{2} \in \mathbb{Z}_{11}^*$. وبالتالى فإن $\overline{2}X-\overline{10} \in \mathbb{Z}_{11}[X]$ غير قابلة للتبسيط .

مثال ٢ : هل يمكنك أن توجد عناصر تشارك كثيرة الحدود $2X-7$ فى : $\mathbb{Z}[X]$ ، $\mathbb{Q}[X]$ ، $\mathbb{Z}_{11}[X]$ ؟

الحل : فى $\mathbb{Z}[X]$ توجد وحدتان فقط هما 1+ ، 1- . وبالتالى فإنه فى $\mathbb{Z}[X]$ $2X-7$ يشارك فقط فى $-2X+7$

فى $\mathbb{Q}[X]$ جميع عناصر $\mathbb{Q}^*$ وحدات وبالتالى فإنه $q(2X-7) = 2qX-7q,\ q \in \mathbb{Q}^*$ كلها تشارك $2X-7$

كذلك فى $\mathbb{Z}_{11}[X]$: $\mathbb{Z}_{11}$ حقل وبالتالى كل عنصر فى $\mathbb{Z}_{11}^*$ يكون وحدة ومن ثم فإن :

$\bar{k}(\bar{2}X-\bar{7})=\overline{2k}X-\overline{7k}\in\mathbb{Z}_{11}[X],\ \bar{k}\in\mathbb{Z}_{11}^{*}$ كلها تشارك $\bar{2}X-\bar{7}$. على سبيل المثال $\bar{4}X-\bar{3}=\bar{2}(\bar{2}X-\bar{7})$ يشارك $\bar{2}X-\bar{7}$ فى $\mathbb{Z}_{11}[X]$.

مثال ٣ : اوجد جميع وحدات $\mathbb{Z}[i]$

الحل : كما نعلم $\mathbb{Z}[i]:=\{m+ni\in\mathbb{C}\mid m,n\in\mathbb{Z}\}$

نعتبر

$$\mu:\mathbb{Z}[i]\to\mathbb{N}$$
$$m+ni\mapsto m^2+n^2$$

(سنستخدم هذا الراسم فى أمثلة تالية)

كما جاء فى (٣-٢-١٠) سيكون

$$\forall x,y\in\mathbb{Z}[i]:\mu(xy)=\mu(x)\mu(y)$$

إذا كانت $m_1+n_1i\in\mathbb{Z}[i]$ وحدة فإنه توجد $m_2+n_2i\in\mathbb{Z}[i]$ وحدة بحيث يكون

$$(m_1+n_1i)(m_2+n_2i)=1$$

وهذا يستلزم أن

$$\mu(m_1+n_1i)\mu(m_2+n_2i)(=\mu((m_1+n_1i)(m_2+n_2i)))=\mu(1)$$

أى أن

$$(m_1^2+n_1^2)(m_2^2+n_2^2)=1\underset{m_1,m_2,n_1,n_2\in\mathbb{Z}}{\Rightarrow}m_1^2+n_1^2=1\Rightarrow m_1=\pm1,\ n_1=0 \text{ أو } m_1=0,\ n_1=\pm1,$$

أى أن وحدات $\mathbb{Z}[i]$ هى : ±1 ، $\pm i$.

مثال ٤ : برهن أو انف :

كل عنصر قابل للتبسيط فى $\mathbb{Z}$ يكون قابلاً للتبسيط فى $\mathbb{Z}[i]$

الحـل : التقرير خاطئ . $5\in\mathbb{Z}$ غير قابل للتبسيط بينما $5=(1+2i)(1-2i)\in\mathbb{Z}[i]$ ، من مثال٣ السابق مباشرة $1\pm2i\in\mathbb{Z}[i]$ ليس وحدة ، وبالتالى فإن $5\in\mathbb{Z}[i]$ قابل للتبسيط .

مثال ٥ : برهن على أن 6 لايمكن أن تكتب بطريقة وحيدة (بدون حساب التشاركات (up to associates)) كحاصل ضرب عناصر غير قابلة للتبسيط فى $\mathbb{Z}[\sqrt{-5}]$

الحل : $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$

سنثبت أن $1+\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ غير قابل للتبسيط .

إذا كان $1+\sqrt{-5} = xy$ حيث $x, y \in \mathbb{Z}[\sqrt{-5}]$ فإن :

$$\mu(x)\mu(y) = \mu(xy) = \mu(1+\sqrt{-5}) = 26 \Rightarrow \mu(x) \in \{1,2,13,26\}$$

$\mu(x)=1 \Leftarrow x$ وحدة (رأينا فى(٣-٢-١٠) أنه توجد وحدتان فقط فى $\mathbb{Z}[\sqrt{-5}]$ هما ± 1) .

$\mu(x) = 26 \Leftarrow \mu(y) = 1 \Leftarrow y$ وحدة .

$\mu(x) = 2 \Leftarrow \alpha^2 + 5\beta^2 = 2$ لبعض $\alpha, \beta \in \mathbb{Z}$ ، وهذا غير ممكن .

$\mu(x) = 13 \Leftarrow \alpha^2 + 5\beta^2 = 13$ لبعض $\alpha, \beta \in \mathbb{Z}$: أيضاً غير ممكن

إذن $1+\sqrt{-5}$ غير قابل للتبسيط فى $\mathbb{Z}\sqrt{-5}$

سنثبت كذلك أن $2 \in \mathbb{Z}\sqrt{-5}$ غير قابل للتبسيط .

إذا كان $2 = xy$ حيث $x, y \in \mathbb{Z}\sqrt{-5}$ فإن :

$$\mu(x)\mu(y) = \mu(xy) = \mu(2) = 4 \Rightarrow \mu(x) \in \{1,2,4\}$$

$\mu(x) = 1 \Leftarrow x$ وحدة فى $\mathbb{Z}\sqrt{-5}$

$\mu(x) = 4 \Leftarrow y$ وحدة فى $\mathbb{Z}\sqrt{-5}$

$\mu(x) = 2 \Leftarrow \alpha^2 + 5\beta^2 = 2$ لبعض $\alpha, \beta \in \mathbb{Z}$ ، وهذا غير ممكن . إذن $2 \in \mathbb{Z}\sqrt{-5}$ غير قابل للتبسيط .

بالمثل $3, 1-\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ غير قابلين للتبسيط .

نهاية البرهان .

مثال ٦ : اختبر إذا ما كانت العناصر الآتية غير قابلة للتبسيط فى $\mathbb{Z}[i]$

(أ) 5 (ب) 7 (جـ) $4+3i$ (د) $6-7i$

الحل : (أ) ليكن $5 = xy$ حيث $x, y \in \mathbb{Z}$ ، $x = a+bi$ ، $y = c+di$

$\Rightarrow 25 = \mu(xy) = \mu(x)\mu(y) \Rightarrow \mu(x) \in \{1,5,25\}$

$\mu(x) = 1 \Rightarrow \mathbb{Z}[i]$ وحدة فى x

$\mu(x) = 25 \Rightarrow \mu(y) = 1 \Rightarrow \mathbb{Z}[i]$ وحدة فى y

$\mu(x) = 5 \Leftrightarrow \mu(y) = 5 \Rightarrow |x|^2 = a^2 + b^2 = 5, |y|^2 = c^2 + d^2 = 5$

$\Rightarrow \quad a = \pm 2, b = \pm 1$ أو $a = \pm 1, b = \pm 2$ ، $c = \pm 2, d = \pm 1$ أو $c = \pm 1, d = \pm 2$

وبسهولة يمكن الاستدلال على أن :

$5 = (2+i)(2-i)$

أو أن

$5 = (1+2i)(1-2i)$

ولا يعنى هذا أن هناك تحليلين مختلفين لــ 5 فى $\mathbb{Z}[i]$ (وسنعلم فى (٣-٣) أن هذا لايمكن أن يحدث فى $\mathbb{Z}[i]$) لأن

$(2+i)(2-i) = i(-2i+1)i(-2i-1) = (1-2i)(1+2i)$

حيث i وحدة فى $\mathbb{Z}[i]$

ومن حيث إن $1+2i, 1-2i \notin (\mathbb{Z}[i])^*$ ، أى ليسا وحدتين فى $(\mathbb{Z}[i])^*$ (مثال٣ السابق) ، فيكون 5 قابلاً للتبسيط فى $\mathbb{Z}[i]$

(ب) ليكن $7 = xy$ حيث $x, y \in \mathbb{Z}[i]$ ، $x = a + bi$ ، $y = c + di \quad \Leftarrow$

$49 = \mu(xy) = \mu(x)\mu(y) \Rightarrow \mu(x) \in \{1,7,49\}$

$\mu(x) = 1 \Rightarrow x \in \mathbb{Z}[i]$ وحدة

$\mu(x) = 49 \Rightarrow \mu(y) = 1 \Rightarrow y \in \mathbb{Z}[i]$ وحدة

$\mu(x) = 7 \Rightarrow |x^2| = a^2 + b^2 = 7, a, b \in \mathbb{Z}$

لايوجد $a, b \in \mathbb{Z}$ بحيث يكون $a^2 + b^2 = 7$

إذن 7 غير قابل للتبسيط فى $\mathbb{Z}[i]$.

(جـ) ليكن $4+3i=xy$ حيث $x,y\in\mathbb{Z}[i]$ ، $x=a+bi$ ، $y=c+di$

$\Rightarrow 25=\mu(xy)=\mu(x)\mu(y)\Rightarrow \mu(x)\in\{1,5,25\}$

$\mu(x)=1\Rightarrow x\in\mathbb{Z}[i]$ وحدة

$\mu(x)=25\Rightarrow \mu(y)=1\Rightarrow y\in\mathbb{Z}[i]$ وحدة

$\mu(x)=5\Leftrightarrow \mu(y)=5\Rightarrow 5=|x^2|=a^2+b^2, 5=|y|^2=c^2+d^2$

حيث $a,b,c,d\in\mathbb{Z}$

$\Rightarrow\quad a=\pm2, b=\pm1$ أو $a=\pm1, b=\pm2$, $c=\pm2, d=\pm1$ أو $c=\pm1, d=\pm2$

ويمكن هنا كذلك الاستدلال بسهولة على أن :

$4+3i=(1+2i)(2-i)$

ومن حيث إن $1+2i$ ،$2-i$ ليسا وحدتين فى $\mathbb{Z}[i]$ ، فيكون $4+3i$ قابلاً للتبسيط فى $\mathbb{Z}[i]$.

(د) ليكن $6-7i=xy$ حيث $x,y\in\mathbb{Z}[i]$

$\Rightarrow 85=\mu(xy)=\mu(x)\mu(y)\Rightarrow \mu(x)\in\{1,5,17,85\}$

$\mu(x)=1\Rightarrow x\in\mathbb{Z}[i]$ وحدة

$\mu(x)=85\Rightarrow \mu(y)=1\Rightarrow y\in\mathbb{Z}[i]$ وحدة

$\mu(x)=5\Leftrightarrow \mu(y)=17\Rightarrow 5=|x^2|=a^2+b^2, 17=c^2+d^2$

حيث $a,b,c,d\in\mathbb{Z}$ ، ($x=a+bi$ ، $y=c+di$)

$\Rightarrow\quad a=\pm2, b=\pm1$ أو $a=\pm1, b=\pm2$ ، $c=\pm4, d=\pm1$ أو $c=\pm1, d=\pm4$

وكذلك نستدل هنا بسهولة على أن :

$6-7i=(4+i)(1-2i)$

ومن حيث إن $1-2i$ ، $4+i$ ليسا وحدتين فى $\mathbb{Z}[i]$ ، فيكون $6-7i$ قابلاً للتبسيط فى $\mathbb{Z}[i]$.

<u>مثال ٧</u> : ليكن D نطاقاً متكاملاً . يقال للراسم $N:D\to\mathbb{Z}$ إنه <u>**معيار ضربى على D**</u> (multiplicative norm on D) إذا حقق الشروط :

(أ) لجميع $\alpha \in D$: $N(\alpha) \geq 0$ ، $N(\alpha) = 0$ إذا كان وفقط إذا كان $\alpha = 0$

(ب) لجمع $\alpha, \beta \in D$: $N(\alpha\beta) = N(\alpha)N(\beta)$

برهن على أنه إذا كان D نطاقاً متكاملاً مع معيار ضربى N فإن $N(1) = 1$ ، لجميع الوحدات $u \in D$ يكون $N(u) = 1$. وإذا كان لجميع $\alpha \in D$: $N(\alpha) = 1$ فإن α تكون وحدة فى D ، عندئذ فإن لكل $\pi \in D$ بحيث إن $N(\pi) = p$ ، $p \in \mathbb{Z}$ عدد أولى يكون π غير قابل للتبسيط فى D .

<u>البرهان</u> :

$$N(1) = N(1.1) = N(1)N(1) \quad \Rightarrow \quad N(1) = 1$$

D نطاق متكامل

وإذا كان $u \in D$ وحدة فإنه يوجد $u^{-1} \in D$ بحيث إن $1 = u^{-1}u$. والآن :

$$1 = N(1) = N(u^{-1}u) = N(u^{-1})N(u)$$

ولأن $N(u)$ عدد صحيح موجب فإن $N(u) = 1$

والآن ليكن $\pi \in D$ بحيث إن $N(\pi) = p$ ، $p \in \mathbb{Z}$ عدد أولى .

ليكن $\pi = \alpha\beta$ حيث $\alpha, \beta \in D$. لدينا

$$p = N(\pi) = N(\alpha\beta) = N(\alpha)N(\beta)$$

هذا يقتضى إما أن يكون $N(\alpha) = 1$ وإما أن يكون $N(\beta) = 1$. ومن الفرض هذا يعنى أنه إما أن يكون α وحدة فى D وإما أن يكون β وحدة فى D . أى أن π غير قابل للتبسيط فى D .

<u>مثال ٨</u> : حدد إذا ما كانت التقارير الآتية صحيحة أم خاطئة :

(أ) إذا كان F حقلاً ، فإن N المعرف كالآتى :

$$N(f(X)) = \deg(f(X))$$

يكون معياراً ضربياً على $F[X]$

(ب) ليكن F حقلاً ، وليكن N معرفاً كالآتى :

$N(f(X)) = 2^{\deg(f(X))}$

لجميع $f(X) \neq 0$ ، $N(0) = 0$. N معيار ضربى على $F[X]$.

الحل : (أ) خاطئ   (ب) صحيح .

مثال ٩ : ليكن D نطاقاً متكاملاً مع معيار ضربى N ، بحيث إن $N(\alpha) = 1$ إذا كان وفقط إذا كان α وحدة فى D. لتكن π بحيث إن : $N(\pi) = \min\{N(\beta) \mid N(\beta) > 1, \beta \in D\}$. برهن على أن π غير قابلة للتبسيط فى D .

البرهان : لتكن π قابلة للتبسيط فىD . إذن يوجد $\alpha, \beta \in D$ ، $\alpha, \beta \notin D^*$ ، $\alpha \neq 0 \neq \beta$: $\pi = \alpha\beta$. هذا يستلزم أن : $N(\pi) = N(\alpha\beta) = N(\alpha)N(\beta)$.

$0 \neq \alpha, \beta \notin D^*$ هذا يستلزم أن $N(\alpha) > 1$ ، $N(\beta) > 1$ ($N(x) \geq 0$ لجميع $x \in D$ ، $N : D \to \mathbb{Z}$ ، $\alpha \in D^* \Leftrightarrow N(\alpha) = 1$) وبالتالى فإن $N(\pi) > N(\alpha) > 1$: تناقض .

مثال ١٠ : برهن على أن $1 + i \in \mathbb{Z}[i]$ غير قابل للتبسيط .

البرهان : ليكن $\begin{aligned} N : \mathbb{Z}[i] &\to \mathbb{Z} \\ a + bi &\mapsto a^2 + b^2 \end{aligned}$. N معيار ضربى ، $u \in \{\pm 1, \pm i\} \Leftrightarrow N(u) = 1$ وهى بالضبط وحدات $\mathbb{Z}[i]$ ، $N(1 + i) = 2$ ، 2 عدد أولى فى $\mathbb{Z}$.

من مثال ٧ السابق ينتج أن $1 + i$ غير قابل للتبسيط فى $\mathbb{Z}[i]$.

طريقة أخرى : استخدم الطريقة السابقة $1 + i = xy$ ، حيث $x, y \in \mathbb{Z}[i]$ ، $2 = \mu(1 + i) = \mu(xy) = \mu(x)\mu(y)$ ، وأكمل ...

مثال ١١ : ليكن $n \in \mathbb{N}$ ، لا يقبل القسمة على مربع أى عدد أولى . لتكن

$$\mathbb{Z}[\sqrt{-n}] := \{a + ib\sqrt{n} \mid a, b \in \mathbb{Z}\}$$

(أ) برهن على أن N المعرف $N(\alpha) = a^2 + nb^2$ حيث $\alpha = a + ib\sqrt{n}$ هو معيار طبيعى.

(ب) برهن على أن $N(\alpha) = 1 \Leftrightarrow \alpha \in \mathbb{Z}[\sqrt{-n}]$ وحدة .

البرهان : (أ) واضح أن $N(\alpha) \geq 0$ ، $N(\alpha) = 0 \Leftrightarrow a = b = 0 \Leftrightarrow \alpha = 0$

ليكن $\alpha = a + ib\sqrt{n}$ ، $\beta = c + id\sqrt{n}$ ينتج أن :

$\alpha\beta = ac - nbd + i(ad+bc)\sqrt{n}$

$\Rightarrow N(\alpha\beta) = (ac-nbd)^2 + (ad+bc)^2 n$

$= a^2c^2 + n^2b^2d^2 + a^2d^2n + b^2c^2n = (a^2+b^2n)(c^2+d^2n)$

$= N(\alpha)N(\beta)$

(ب) لتكن $\alpha = a + ib\sqrt{n}$: $N(\alpha)=1 \Leftrightarrow a^2+nb^2=1 \Leftrightarrow (a+ib\sqrt{n})(a-ib\sqrt{n})=1$

$\Leftrightarrow \alpha = a+ib\sqrt{n} \in (\mathbb{Z}[\sqrt{-n}])^*$

<u>مثال ١٢</u> : أجر ماسبق أن أجريته فى مثال ١١ إذا كانت الحلقة هى :

$\mathbb{Z}[\sqrt{n}] = \{a+b\sqrt{n} \mid a,b \in \mathbb{Z}\}$

وكان $N(\alpha) = |a^2 - nb^2|$ حيث $\mathbb{Z}[\sqrt{n}] \ni \alpha = a+b\sqrt{n}$

<u>البرهان</u> : (أ) ليكن $\alpha = a+b\sqrt{n}$ ، $\beta = c+d\sqrt{n} \Leftarrow$

$\alpha\beta = (a+b\sqrt{n})(c+d\sqrt{n}) = ac+nbd+(ad+bc)\sqrt{n}$

$\Rightarrow N(\alpha\beta) = |(ac+nbd)^2 - n(ad+bc)^2|$

$= |a^2c^2 + n^2b^2d^2 - na^2d^2 - nb^2c^2|$

$= |a^2-nb^2||c^2-nd^2| = N(\alpha)N(\beta)$

واضح أن $N(\alpha) = |a^2-nb^2| \geq 0$ ، $a^2-nb^2=0$ إذا كان وفقط إذا كان

$a+b\sqrt{n}=0$ أو $a-b\sqrt{n}=0 \Leftrightarrow (a+b\sqrt{n})(a-b\sqrt{n})=0$

$\alpha = a+b\sqrt{n}=0 \Leftrightarrow b=0$ ، $a=0 \quad \Leftrightarrow$

(ب)

$N(\alpha)=1 \Leftrightarrow |a^2-nb^2|=1 \Leftrightarrow a^2-nb^2=\pm 1$

$\Leftrightarrow (a+\sqrt{n}b)(a-\sqrt{n}b)=\pm 1$

إذا كان $(a+b\sqrt{n})(a-b\sqrt{n}b)=1$ فإن $a+b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ يكون وحدة

وإذا كان $(a+b\sqrt{n})(a-b\sqrt{n}b)=-1$ فإن $(a+b\sqrt{n})(-a+b\sqrt{n})=1$

ويكون $a+b\sqrt{n}\in\mathbb{Z}[\sqrt{n}]$ كذلك وحدة .

<u>مثال ١٣</u> : برهن على أن العنصر $\sqrt{-5}$ هو عنصر أولى فى النطاق المتكامل $\mathbb{Z}[\sqrt{-5}]$

<u>البرهان</u> : إذا كان $\sqrt{-5}\mid(a+b\sqrt{-5})(c+d\sqrt{-5})$ حيث $a,b,c,d\in\mathbb{Z}$

فإنه يوجد $x+y\sqrt{-5}$ حيث $x,y\in\mathbb{Z}$ بحيث يكون

$$(a+b\sqrt{-5})(c+d\sqrt{-5})=\sqrt{-5}(x+y\sqrt{-5}) \qquad (1)$$

وبوضع $-\sqrt{-5}$ بدلاً من $\sqrt{-5}$ فى (1) (لماذا يكون هذا جائزاً ؟)

نحصل على :

$$(a-b\sqrt{-5})(c-d\sqrt{-5})=-\sqrt{-5}(x-y\sqrt{-5}) \qquad (2)$$

من (1) ، (2) نحصل على :

$$(a^2+5b^2)(c^2+5d^2)=5(x^2+5y^2)$$

أى أن :

$$5\mid(a^2+5b^2)(c^2+5d^2)$$

أى أن :

$$5\mid a^2c^2+5a^2d^2+5b^2c^2+25b^2d^2)$$

ولكن

$$5\mid 5a^2d^2+5b^2c^2+25b^2d^2$$

وهكذا فإن :

$$5\mid a^2c^2$$

5 عدد أولى فى $\mathbb{Z}$ فينتج أن $5\mid a^2$ أو $5\mid c^2$

$5\mid a^2$ يستلزم أن $5\mid a$ لأن 5 عدد أولى فى $\mathbb{Z}$.

$5 \mid c^2$ يستلزم أن $5 \mid c$ (كان يمكن الحصول على هذا مباشرة من $5 \mid aacc$ ، 5 عدد أولى فى $\mathbb{Z}$)

$5 \mid a$ يستلزم أن $\sqrt{-5} \mid a$ فى $\mathbb{Z}[\sqrt{-5}]$ لأن $5 = (\sqrt{-5})(-\sqrt{-5})$

وفى هذه الحالة يكون $\sqrt{-5} \mid (a+\sqrt{-5}b)$

$5 \mid c$ يستلزم كذلك أن $\sqrt{-5} \mid c$

وفى هذه الحالة يكون $\sqrt{-5} \mid (c+\sqrt{-5}d)$

أى أن $\sqrt{-5}$ عنصر أولى فى $\mathbb{Z}[\sqrt{-5}]$

طريقة أخرى : ليكن $\sqrt{-5} \mid (a+b\sqrt{-5})(c+d\sqrt{-5})$

حيث $a,b,c,d \in \mathbb{Z}$. ينتج أن :

$$\sqrt{-5} \mid [ac-5bd+\sqrt{-5}(ad+bc)]$$

$$\Rightarrow \sqrt{-5} \mid ac-5bd \Rightarrow \sqrt{-5} \mid ac \Rightarrow 5 \mid a^2c^2$$

وأكمل كما سبق .

<u>**مثال ١٤**</u> : برهن على أن $21 \in \mathbb{Z}[\sqrt{-5}]$ يمكن أن يكتب على صورة حاصل ضرب عناصر غير قابلة للتبسيط بأكثر من طريقة (بدون حساب التشاركات)

<u>**البرهان**</u> : $21 = 3.7 = (1-2\sqrt{-5})(1+2\sqrt{-5})$

يترك للقارئ البرهنة على أن 3 ، 7 ، $1 \pm 2\sqrt{-5}$ غير قابلة للتبسيط فى $\mathbb{Z}[\sqrt{-5}]$ (انظر مثال٥ السابق)

<u>**مثال ١٥**</u> : برهن على أن $1+3\sqrt{-5}$ غير قابل للتبسيط ، لكنه غير أولى فى $\mathbb{Z}[\sqrt{-5}]$.

<u>**البرهان**</u> : سنبرهن أولاً على أن $1+3\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ غير قابل للتبسيط . ليكن $x,y \in \mathbb{Z}[\sqrt{-5}]$ ، $1+3\sqrt{-5} = xy$. ينتج أن :

$$\mu(xy) = \mu(x)\mu(y) = 1+(9)(5) = 46 = (2)(23)$$

(تعريف μ كما جاء فى (٣-٢-١٠))

$$\Rightarrow \mu(x) \in \{1, 2, 23, 46\}$$

ليكن $x = a + b\sqrt{-5}$ فإنه إذا كان $\mu(x) = 2$ فإن : $a^2 + 5b^2 = 2$

ولاتوجد أعداد a ، b فى $\mathbb{N}$ تحقق هذه المعادلة .

كذلك إذا كان $\mu(x) = 23$ فإنه لايوجد كذلك $a, b \in \mathbb{N}$ بحيث يكون $a^2 + 5b^2 = 23$

إذا كان $\mu(x) = 1$ فمعنى هذا أن x وحدة . أما إذا كان $\mu(x) = 46$ فإن $\mu(y) = 1$

وهذا معناه أن y وحدة .

إذن $1 + 3\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ غير قابل للتبسيط

نبرهن الآن على أن العنصر المعنى ليس أولياً .

نلاحظ أن $(1 + 3\sqrt{-5})(1 - 3\sqrt{-5}) = 46 = (2)(23)$

سنبرهن الآن على أن $1 + 3\sqrt{-5}$ ليس قاسماً لـ 2 ، وليس قاسماً لـ 23 على الرغم من أنه قاسم لحاصل ضربهما وبهذا يكون غير أولى .

ليكن $(1 + 3\sqrt{-5})(x + y\sqrt{-5}) = 2$ حيث $x, y \in \mathbb{Z}$. ينتج أن :

$$x - 15y + (3x + y)\sqrt{-5} = 2$$

$$\Rightarrow x - 15y = 2, 3x + y = 0 \Rightarrow 45y + 6 + y = 0 \Rightarrow y = \frac{-3}{23}$$

وهذا مستحيل (لأن $y \in \mathbb{Z}$)

ليكن $(1 + 3\sqrt{-5})(x + y\sqrt{-5}) = 23$ حيث $x, y \in \mathbb{Z}$. ينتج أن :

$$x - 15y = 23, 3x + y = 0 \Rightarrow 45y + 69 + y = 0 \Rightarrow y = \frac{-3}{2}$$

وهذا أيضاً مستحيل .

نهاية البرهان .

مثال ١٦ : ليكن F حقلاً ، وليكن $p(X),a(X),b(X)\in F[X]$. إذا كان $p(X)$ غير قابل للتبسيط على $F[X]$ ، وكان $p(X)|a(X)b(X)$ ، عندئذ فإن $p(X)|a(X)$ أو $p(X)|b(X)$

البرهان : لأن $p(X)$ غير قابل للتبسيط فى (على) $F[X]$ فإن $[p(X)]$ يكون مثالياً أعظم فى $F[X]$ (نتيجة (٣-٢-٩)) ، ومن النظرية (١-٣-١١) يكون $F[X]/[p(X)]$ حقلاً . ومن ثم فهو نطاق متكامل . والآن لدينا الإبيمورفيزم الطبيعى :

$$\varphi: F[X]\to F[X]/[p(X)]$$
$$f(X)\mapsto f(X)+[p(X)]$$

ليكن $\varphi(a(X))=a(X)+[p(X)]=\overline{a(X)}$ ، $\varphi(b(X))=b(X)+[p(X)]=\overline{b(X)}$

ولأن $p(X)|a(X)b(X)$ فإنه يوجد $q(X)$ بحيث يكون $a(X)b(X)=p(X)q(X)$ وبالتالى فإن :

$$\overline{a(X)}\ \overline{b(X)}=\overline{a(X)b(X)}=a(X)b(X)+[p(X)]$$
$$=[p(X)]=\overline{0}$$

ولأن $F[X]/[p(X)]$ نطاق متكامل فإن $\overline{a(X)}=\overline{0}$ أو $\overline{b(X)}=\overline{0}$

أى أن $a(X)+[p(X)]=[p(X)]$ أو $b(X)+[p(X)]=[p(X)]$ وبالتالى فإن $a(X)\in[p(X)]$ أو $b(X)\in[p(X)]$ ومن ثم فإن $p(X)|a(X)$ أو $p(X)|b(X)$.

مثال ١٧ : ليكن F حقلاً ، $p(X)$ عنصراً غير قابل للتبسيط (للتحليل) فى $F(X)$. إذا كان E حقلاً يحتوى F ، وكان هناك عنصر $a\in E$ بحيث إن $p(a)=0$ ، فبرهن على أن الراسم

$$\varphi: F[X]\to E$$
$$f(X)\mapsto f(a)$$

هومومورفيزم حلق ، وأن نواته هى $[p(X)]$

البرهان :

$$\forall f(X),g(X)\in F[X]:$$

$$\varphi(f(X)+g(X))=\varphi((f+g)(X))=(f+g)(a)=f(a)+g(a)$$
$$=\varphi(f(X))+\varphi(g(X))$$

$$\varphi(f(X)g(X))=\varphi((fg)(X))=(fg)(a)=f(a)g(a)=\varphi(f(X))\varphi(g(X))$$

$$\varphi(1) = 1(a)=1$$

كثيرة الحدود 1

أى أن φ هومومورفيزم حلق .

$$Ker(\varphi)=\{f(X)\in F[X] \mid f(a)=0\}$$

وهو مثالى . واضح أن $p(X)\in Ker(\varphi)$ ومن ثم فإن $[p(X)]\subset Ker(\varphi)$.

لكن $p(X)$ غير قابل للتبسيط فى $F[X]$ وبالتالى فإن $[p(X)]$ مثالى أعظم فى $F[X]$ (النتيجة (٣-٢-٩)) ،

ومن ثم فإن $[p(X)]=Ker(\varphi)$.

<u>**مثال ١٨**</u> : برهن على أنه إذا كان p عدداً أولياً فى $\mathbb{Z}$ بحيث يمكن كتابته على الصورة a^2+b^2 ، عندئذ فإن $a+bi$ يكون غير قابل للتبسيط فى $\mathbb{Z}[i]$. اوجد ثلاثة أعداد أولية يكون لها هذه الخاصة، واوجد العناصر غير القابلة للتبسيط المناظرة .

<u>**الحل**</u> : ليكن

$$\mu:\mathbb{Z}[i]\to\mathbb{N}$$
$$a+bi\mapsto a^2+b^2=p$$

ليكن $a+bi=xy$ حيث $x,y\in\mathbb{Z}[i]$. لدينا

$$a+bi=xy\Rightarrow \mu(x)\mu(y)=\mu(xy)=\mu(a+ib)=a^2+b^2=p$$
$$\Rightarrow \quad \mu(x)=1 \quad \text{أو} \quad \mu(y)=1$$

p عدد أولى

أى أن x أو y وحدة فى $\mathbb{Z}[i]$. وبالتالى فإن $a+bi$ يكون غير قابل للتبسيط فى $\mathbb{Z}[i]$.

2 عدد أولى له هذه الخاصة وعنصر غير قابل للتبسيط مناظر هو $1+i$. (يصلح كذلك $1-i$) كذلك 5 عدد أولى به نفس الخاصة ، $1+2i$ عنصر غير قابل للتبسيط مناظر ، 13 عدد أولى له نفس الخاصة ، $3+2i$ عنصر غير قابل للتبسيط مناظر .

<u>مثال ١٩</u> : ليكن D نطاقاً إقليدياً ، d هو الراسم المصاحب . برهن على أنه إذا كان $a,b\in D$ متشاركيين (associate) فإن $d(a)=d(b)$ بفرض أن d يحقق : لكل عنصرين غير صفرين

$$d(a)\le d(ab)\ :\ a,b\in D$$

<u>البرهان</u> : $a,b\in D$ يتشاركان يقتضى وجود وحدتين $u,v\in D$ بحيث إن: $a=bu$ (1) ، $b=av$ (2) ، $u\,v=1$. والآن من (١) لدينا : $d(a)=d(bu)\ge d(b)$ (3)

ومن (2) لدينا : (4) $d(b)=d(av)\ge d(a)$. من (3) ، (4) ينتج المطلوب مباشرة .

ملحوظة : بعض المراجع تضع هذا الفرض الذى ذكرناه ضمن تعريف النطاق الإقليدى . انظر مثال ٣١ فى (٢-٢-٨) .

<u>مثال ٢٠</u> : ليكن D نطاقاً متكاملاً ، وليكن $p,q\in D$ عنصرين غير قابلين للتبسيط وليكن (p) مجموعة جميع العناصر المتشاركة مع p وبالمثل (q) : برهن على أن

$$(p)\cap(q)\ne\phi\Rightarrow(p)=(q)$$

<u>البرهان</u> :

$$(p)\cap(q)\ne\phi\Rightarrow\exists s\in D: s=pu=qv\,;u,v\in D^*\quad \text{(وحدتان)}$$

$$x\in(p)\Rightarrow\exists w\in D^*: x=pw=qvu^{-1}w\in(q)\Rightarrow(p)\subset(q)$$

(حاصل ضرب وحدتين = وحدة)

بالمثل $(q)\subset(p)$ وينتج المطلوب مباشرة .

تمارين

(١) صف العناصر غير القابلة للتبسيط فى $R[X]$ حيث R نطاق تحليل وحيد بدلالة العناصر غير القابلة للتبسيط فى R ، العناصر غير القابلة للتبسيط فى $Q[X]$ حيث Q هو حقل القسمة لـــ R . هل هناك صفة أخرى لهذه العناصر ؟ (انظر (٣-٣-٢))

(٢) حلل $X^3 - Y^3$ إلى عناصر غير قابلة للتبسيط فى $\mathbb{Q}[X ,Y]$ ، وبرهن على أن كل عامل يكون غير قابل للتبسيط .

(٣) كرر المطلوب فى (٢) بالنسبة لكثيرة الحدود $X^3 + Y^3$

(٤) كرر المطلوب فى (٢) بالنسبة لكثيرة الحدود $X^2 + Y^2$

(إرشاد: تستطيع الاستعانة بنتيجة (٣-٥-٧) التى ستأتى فيما بعد ، ومعرفة أن $\mathbb{Z}$ "نطاق تحليل وحيد " كما سيأتى ، والنتيجة (٣-٥-١٠) التى ستأتى كذلك) .

(٥) ليكن F حقلاً ، ولتكن $p(X),a_1(X),a_2(X),...,a_k(X)\in F[X]$ حيث $p(X)$ عنصر غير قابل للتبسيط . إذا كان $p(X)\mid a_1(X)a_2(X)..a_k(X)$ ، فبرهن على أن $p(X)$ يقسم $a_i(X)$ لبعض i .

(هذا التمرين تعميم لمثال ١٦ فى (٣-٢-١١) . ولكن المطلوب حله بطريقة مختلفة عن حل المثال !).

(٦) ليكن F حقلاً . برهن على أن كل مثالى أولى فى $F[X]$ يكون مثالياً أعظم

(٧) برهن على أن $\mathbb{Z}[i]/_{[3]}$ ليس متشاكلا حلقيا مع $\mathbb{Z}_3 \otimes \mathbb{Z}_3$

(إرشاد: $\mathbb{Z}[i]$ نطاق متكامل ذو عنصر وحدة ،$3\in\mathbb{Z}[i]$ عنصر أولى ، وبالتالى فإن $[3]$ مثالى أولى فى $\mathbb{Z}[i]$. $\mathbb{Z}[i]$ نطاق إقليدى وبالتالى فإنه نطاق مثاليات أساسية ويكون $[3]$ مثالياً أعظم فيه. ومن ثم فإن $\mathbb{Z}[i]/_{[3]}$حقل. $\mathbb{Z}_3\otimes\mathbb{Z}_3$ ليس حقلاً . لماذا ؟ واملأ التفصيلات)

(٨) برهن على أنه فى $\mathbb{Z}[i]$: 3 غير قابل للتبسيط ، 2 قابل للتبسيط

(٩) فى أى نطاق متكامل برهن على أن حاصل ضرب عنصر غير قابل للتبسيط فى وحدة يكون عنصراً غير قابل للتبسيط .

(١٠) برهن على أن $1-i$ غير قابل للتبسيط فى $\mathbb{Z}[i]$

(١١) برهن على أنه فى مثال ١٢ من (٣-٢-١١) إذا كان $N(\alpha)=|a^2-nb^2|$ حيث $\alpha=a+b\sqrt{n}$ ، عدداً أولياً فإن α يكون عنصراً غير قابل للتبسيط فى $\mathbb{Z}[\sqrt{n}]$

(١٢) برهن على أنه فى النطاق المتكامل R إذا كان $a,b\in R$ يتشاركان فإن $[a]=[b]$

(١٣) برهن على أن 7 غير قابل للتبسيط فى $\mathbb{Z}[\sqrt{6}]$ ، على الرغم من أن $N(7)$ ليس أولياً. (وهكذا فإن عكس التقرير فى تمرين (١١) السابق ليس صحيحاً)

(١٤) برهن على أن 2 ، $1+\sqrt{5}$ غير قابلين للتبسيط فى $\mathbb{Z}[\sqrt{5}]$

(١٥) ليكن α عدداً صحيحاً أصغر من 1 - ، ولايقبل القسمة على مربع أى عدد أولى . برهن على أن الوحدات الوحيدة فى $\mathbb{Z}[\sqrt{\alpha}]$ هى 1 ، 1 - .

(١٦) ليكن $a,b\in\mathbb{Z}[\sqrt{\alpha}]$ ، حيث α عدد صحيح لايقبل القسمة على مربع أى عدد أولى ، وكان ab وحدة فى $\mathbb{Z}[\sqrt{\alpha}]$. برهن على أن كلاً من a ، b وحدة .

٣-٣ نطاقات التحليل الوحيد Unique factorization domains

ليكن R نطاقاً متكاملاً . نعتبر التقريرات الآتية :

(ت١) لكل $a\in R$ ، $a\neq 0$ ، $a\notin R^*$ توجد عناصر غير قابلة للتبسيط $q_1,...,q_r\in R$ بحيث إن : $a=q_1...q_r$.

(ت $1''$) لكل $a\in R$ ، $a\neq 0$ ، $a\notin R^*$ توجد عناصر أولية $p_1,...,p_r\in R$ بحيث إن : $a=p_1...p_r$.

(ت٢) إذا كانت q_1 ، ... ، q_r ، q'_1 ، ... ، q'_s عناصر غير قابلة للتبسيط فى R بحيث إن :

$q_1...q_r=q'_1...q'_s$ فإن $r=s$ ، توجد تبديلة $\pi\in\gamma_r(=S_r)$ بحيث إنه لكل $i\in\{1,2,...,r\}$ العناصر q_i ، $q'_{\pi(i)}$ تتشارك .

(ت٣) كل عنصر غير قابل للتبسيط فى R يكون أولياً .

٣-٣-١ نظرية :

ليكن R نطاقاً متكاملاً . التقريرات الآتية متكافئة :

(١) (ت١) ، (ت٢)

(٢) (ت١) ، (ت٣)

(٣) (ت $1''$)

البرهان : (١) $\Leftarrow$ (٢) : للبرهنة على (ت٣) ليكن q عنصراً غير قابل للتبسيط فى R ، وليكن $q\,|\,ab$ حيث $a,b\in R$. عندئذ فإنه يوجد $c\in R$ بحيث إن : $ab=qc$. ومن (ت١) توجد عناصر غير قابلة للتبسيط q_1 ، ... ، q_r ، q'_1 ، ... ، q'_s ، q''_1 ، ... ، q''_t بحيث إن :

$$a=q_1...q_r \text{ ، } b=q'_1...q'_s \text{ ، } c=q''_1...q''_t .$$

بحيث يكون : $q_1...q_r.q'_1...q'_s=qq''_1...q''_t$

ومن (ت٢) يوجد $i \in \{1,2,...,r\}$ بحيث إن $q \sim q_i$ أو يوجد $j \in \{1,2,...,s\}$ بحيث إن $q \sim q'_j$ وبالتالى فإنه ينتج أن $q \mid a$ أو $q \mid b$ ، أى أن q عنصر أولى .

(٢) ⇐ (٣) : واضح .

(٣) ⇐ (١) : من (ت $\bar{1}$) ينتج أن كل عنصر غير قابل للتبسيط يكون أولياً .

لأن : إذا كان $q \in R$ عنصراً غير قابل للتبسيط ، فإنه من (ت $\bar{1}$) توجد عناصر أولية $p_1,...,p_r \in R$ بحيث يكون : $q = p_1...p_r$. ولأن q عنصر غير قابل للتبسيط فإن $r = 1$ ، وبالتالى يكون $q = p_1$.

والآن يمكن أن نبرهن على صحة التقرير (ت٢) كالآتى : ليكن q_1، ....، q_r ، q'_1 ، ....، q'_s عناصر غير قابلة للتبسيط (وبالتالى فهى أولية) فى R بحيث إن :

$q_1...q_r = q'_1...q'_s$. لأن q'_1 عنصر أولى فإنه يقسم أحد هذه الـــ $q_i's$. وبدون أى فقد للعمومية (without any loss of generality) ليكن $q'_1 \mid q_1$ ، وبالتالى فإننا نحصل على $q'_1 \sim q_1$ (لأن كليهما q_1 ، q'_1 غير قابل للتبسيط)، أى أنه يوجد u وحدة فى R بحيث يكون : $q'_2...q'_s = uq_2...q_r$. وبالاستمرار فى هذا الاجراء نحصل على المطلوب .

٣-٣-٢ تعريف :

يقال لنطاق متكامل R إنه نطاق تحليل وحيد (Unique Factorization Domain) (باختصار UFD إذا تحقق أحد (وبالتالى جميع) التقريرات فى النظرية (٣-٣-١) .

٣-٣-٣ ملحوظة :

من المثال (٣-٢-١٠)تكون الحلقة (النطاق المتكامل) $\mathbb{Z}[\sqrt{-5}]$ ليست نطاق تحليل وحيد.

٣-٣-٤ نظرية :

كل نطاق مثاليات أساسية يكون نطاق تحليل وحيد .

البرهان : ليكن R نطاق مثاليات أساسية . نعرف :

$M := \{[a] \mid a \in R, a \neq 0, a \notin R^*,$ a ليس حاصل ضرب عناصر أولية فى R $\}$

سنبرهن أولاً على أن $M=\phi$.

إذا كانت $M \neq \phi$ فإنه يوجد عنصر أعظم فى M بالنسبة للاحتواء (لاحظ أن R نطاق مثاليات أساسية $\Leftarrow R$ نويترية) . ليكن $[d]$ عنصراً أعظم فى M . ينتج من تعريف M ومن (٣-٢-٧ (٢)) أن $[d]$ ليس مثالياً أولياً وهذا يستلزم (من مثال ٢٨ فى (١-٣-٢٠)) أن $[d]$ ليس مثالياً أعظم فى R . ولأن R نطاق مثاليات أساسية فإنه يوجد $b \in R$ بحيث إن $[d] \subsetneq [b] \subsetneq R$. وهذا يستلزم أنه يوجد $c \in R$ بحيث يكون $d = b\,c$ وهذا يقتضى أن $[d]=[bc] \subsetneq [c]$ (لأن : $[b] \neq R$ ومن ثم فإن $b \notin R^*$ وبالتالى فإن $[bc] \neq [c]$)

وهذا يستلزم أن $[b] \notin M$ ، $[c] \notin M$. والآن $b, c \neq 0$ ، وكذلك $b, c \notin R^*$ (لأن $[d] \neq [b]$ ينتج أن $c \notin R^*$) فينتج من تعريف M أن $b = p_1 \ldots p_n$ ، $c = p_1' \ldots p_m'$ حيث p_i ، p_j' عناصر أولية . ولكن هذا يستلزم أن $d = p_1 \ldots p_n p_1' \ldots p_m'$ وهذا تناقض مع فرض أن $[d] \in M$. أى أن $M=\phi$. وينتج المطلوب مباشرة .

<u>٣-٣-٥ نتيجة</u> :

من النظرية (٢-١-٩) كل نطاق إقليدى يكون نطاق مثاليات أساسية ومن النظرية (٣-٣-٤) السابقة مباشرة كل نطاق مثاليات أساسية يكون نطاق تحليل وحيد . أى أن :

R نطاق إقليدى $\Leftarrow R$ نطاق مثاليات أساسية $\Leftarrow R$ نطاق تحليل وحيد

<u>٣-٣-٦ أمثلة محلولة</u> :

<u>مثال١</u> : فى المثال (١) من (٢-١-٨) رأينا أن $\mathbb{Z}$ نطاق إقليدى ، ورأينا قبل ذلك فى المثال(١) من(١-٢-١٣) أن $\mathbb{Z}$ نطاق مثاليات أساسية، وبالتالى فإن $\mathbb{Z}$ نطاق تحليل وحيد.

الكتابة $24 = (2)(2)\,(3)(2) = (-2)\,(-3)\,(2)(2)$

لاتناقض حقيقة أن $\mathbb{Z}$ نطاق تحليل وحيد فالعنصران 2 ، 2- متشاركان ، وكذلك 3 ، 3- . وتغيير ترتيب العناصر لاينقض شيئاً .

ولاحظ أن كل هذا متضمن فى التقرير (ت ٢) السابق .

مثال ٢ : عبر عن كثيرة الحدود f – إن أمكن – فى صورة حاصل ضرب عناصر غير قابلة للتبسيط فى النطاقات المتكاملة الآتية : $\mathbb{Z}[X]$ ، $\mathbb{Q}[X]$ ، $\mathbb{Z}_{11}[X]$:

$$f := 4X^2 - 4X + 8$$

الحل : فى $\mathbb{Z}[X]$: $4X^2 - 4X + 8 = (2)(2)(X^2 - X + 2)$

2 ، $X^2 - X + 2$ غير قابلة للتبسيط فى $\mathbb{Z}[X]$

فى $\mathbb{Q}[X]$: $4X^2 - 4X + 8$ هى نفسها غير قابلة للتبسيط

ويلاحظ أن $2 \in \mathbb{Q}^*[X]$: إذن 2 ليس غير قابل للتبسيط وبالتالى فإن التعبير $4X^2 - 4X + 8 = (2)(2)(X^2 - X + 2) \in \mathbb{Q}[X]$ لايعنى أن f كتبت على صورة حاصل ضرب عناصر غير قابلة للتبسيط .

فى $\mathbb{Z}_{11}[X]$:

$$\bar{4}X^2 - \bar{4}X + \bar{8} = \bar{4}X^2 - \bar{4}X - \bar{3}$$

$$= (\bar{2}X - \bar{3})(\bar{2}X + \bar{1}) \qquad (1)$$

كذلك

$$\bar{4}X^2 - \bar{4}X + \bar{8} = \bar{4}X^2 + \overline{18}X + \bar{8}$$

$$= (\bar{4}X + \bar{2})(X + \bar{4}) \qquad (2)$$

هل التعبيران (1) ، (2) مختلفان ؟

$\mathbb{Z}_{11}$ حقل ، ومن ثم فإن $\mathbb{Z}_{11}[X]$ نطاق إقليدى (وكذلك نطاق مثاليات أساسية) ومن ثم فهو نطاق تحليل وحيد، وبالتالى فإن التعبيرين لايمكن أن يكونا مختلفين ونرى ذلك لأن :

$$\left.\begin{array}{l} \bar{4}X + \bar{2} = \bar{2}(\bar{2}X + \bar{1}) \\ (\bar{2}X - \bar{3}) = \bar{2}(X + \bar{4}) \end{array}\right\}, \bar{2} \in \mathbb{Z}_{11}^*,$$

ولأن $\mathbb{Z}_{11}[X]$ نطاق تحليل وحيد فهو يحقق (ت ٢)

مثال ٣ : حدد إذا ما كانت التقريرات الآتية صحيحة أم خاطئة :

(أ) كل حقل هو نطاق تحليل وحيد

(ب) كل نطاق تحليل وحيد يكون نطاق مثاليات أساسية .

(جـ) $\mathbb{Z}[X]$ نطاق تحليل وحيد

(د) إذا كان D نطاق مثاليات أساسية فإن $D[X]$ يكون نطاق مثاليات أساسية

(هـ) إذا كان D نطاق تحليل وحيد فإن $D[X]$ يكون كذلك نطاق تحليل وحيد

(و) أى نطاق تحليل وحيد لايحتوى على قواسم صفرية .

(ز) فى أى نطاق تحليل وحيد إذا كان $p \mid a$ حيث p غير قابل للتبسيط ، فإن p نفسها تظهر فى كل تحليل لـــ a .

(ح) كل عنصرين غير قابلين للتبسيط فى نطاق تحليل وحيد يكونان متشاركين .

<u>الحل</u> :

(أ) صحيح كما سبق فى مثال ٢٦ من (٢-٢-٨) ، (٣-٣-٤)

(ب) خطأ : $\mathbb{Z}[X]$ نطاق تحليل وحيد لكنه ليس نطاق مثاليات أساسية . (كذلك (جـ) صحيح)

(د) خطأ : $\mathbb{Z}$ نطاق مثاليات أساسية ، لكن $\mathbb{Z}[X]$ ليس نطاق مثاليات أساسية .

(هـ) صحيح

(و) أى نطاق تحليل وحيد هو نطاق متكامل، وبالتالى لايحتوى على أية قواسم صفرية.

(ز) خطأ : مثال مضاد : $\mathbb{Z}[X] \ni 2X+4 = 2(X+2) = (-2)(-X-2)$

-1 وحدة فى $\mathbb{Z}[X]$

(ح) خطأ $2,3 \in \mathbb{Z}$ بينما $3 \neq \pm 2, 2 \neq \pm 3$ حيث ± 1 هما الوحدتان الوحيدتان فى $\mathbb{Z}$.

<u>مثال ٤</u> : اضرب مثالاً لبيان أن كثيرة حدود $g[X]$ فى $D[X]$ حيث D نطاق تحليل وحيد (وبالتالى $D[X]$ نطاق تحليل وحيد) قد تكون قابلة للتبسيط ، بينما هى فى $F[X]$ ، حيث F هو حقل القسمة لـــ D ، غير قابلة للتبسيط .

<u>الحـــل</u> : $\mathbb{Q}[X] \ni g(X) = 2X+4 = 2(X+2)$ غير قابلة للتبسيط لأن $2 \in \mathbb{Q}^*$

بينما $\mathbb{Z}[X] \ni g(X)$ قابلة للتبسيط لأن $2, X+2 \notin (\mathbb{Z}[X])^*$.

مثال ٥ : ليكن D نطاق تحليل وحيد . هل $D\setminus D^*$ (D^* هى مجموعة الوحدات فى D ، كما هو متوقع !) تمثل زمرة بالنسبة للضرب فى D ؟

الحل : على الرغم من أن $D\setminus D^*$ مغلقة (closed) بالنسبة للضرب فى D ، أى أن :

$$\forall x, y \in D\setminus D^* : xy \in D\setminus D^*$$

إلا أن عنصر الوحدة "1" لا ينتمى إلى $D\setminus D^*$ ، لأنه عنصر فى D ، D^* . وبالتالى فإن $D\setminus D^*$ لاتمثل زمرة بالنسبة للضرب فى D .

مثال ٦ : ادرس التحليل إلى عناصر غير قابلة للتبسيط فى $\mathbb{Z}\otimes\mathbb{Z}$. وعلى سبيل الخصوص اعتبر العنصر $(1, 0)$

الحل : ليس كل عنصر غير وحدة (nonunit) ولايساوى الصفر فى $\mathbb{Z}\otimes\mathbb{Z}$ يمكن تحليله إلى عناصر غير قابلة للتبسيط فى $\mathbb{Z}\otimes\mathbb{Z}$

العنصر $(1,0)$ ليس وحدة فى $\mathbb{Z}\otimes\mathbb{Z}$ ، وكل تحليل لهذا العنصر يحتوى على العامل $(\pm1,0)$ ، وهو قابل للتبسيط ، لأن $(\pm1,0)=(\pm1,0)(1,30)$ مثلاً . العناصر غير القابلة للتبسيط فى $\mathbb{Z}\otimes\mathbb{Z}$ هى فقط $(\pm1, p)$ ، $(q,\pm1)$ حيث p ، q عنصران غير قابلين للتبسيط فى $\mathbb{Z}$.

مثال ٧ : برهن على أنه يوجد عدد لا نهائى من الأعداد الأولية .

البرهان : (إقليدس) : لتكن p_1 ، p_2 ، ... ، p_n جميع الأعداد الأولية فى $\mathbb{Z}$. هذا يقتضى أن $0,\pm1 \neq p_1p_2...p_n+1\in\mathbb{Z}$. هذا يقتضى أن $p_1p_2...p_n+1$ له على الأقل قاسم وهو عدد أولى . أى أنه يوجد $1\le i\le n$ بحيث يكون $p_i \mid (p_1p_2...p_n+1)$. ومن $p_i \mid p_1p_2...p_n$ ينتج أن $p_i \mid 1$. تناقض

مثال ٨ : برهن على أن : p عدد أولى فى $\mathbb{Z}$ $\Leftarrow p$ عنصر أولى فى $\mathbb{Z}[i]$ أو يوجد عنصر أولى $\pi\in\mathbb{Z}[i]$ بحيث يكون $p=\pi\bar{\pi}$

البرهان : ليكن p عدداً أولياً فى $\mathbb{Z}$ نعلم من مثال ٣ (٣-٢-١١) أن p ليس وحدة فى $\mathbb{Z}[i]$. ولأن $\mathbb{Z}[i]$ نطاق تحليل وحيد (لماذا ؟) فإنه توجد عناصر أولية $\pi_1,...,\pi_n\in\mathbb{Z}[i]$

بحيث يكون $p = \pi_1 ... \pi_n$. وهذا يقتضى أن $p^2 = p\bar{p} = (\pi_1\bar{\pi}_1)...(\pi_n\bar{\pi}_n)$. على اليمين فى المتساوية السابقة تحليل لـــ p^2 فى عوامل صحيحة كلها > 1 . ولكن $\mathbb{Z}[i]$ نطاق تحليل وحيد فإما أن يكون $n = 1$ ، وفى هذه الحالة يكون $p = \pi_1$ وإما أن يكون $n = 2$ ، $p = \pi_1\bar{\pi}_1 = \pi_2\bar{\pi}_2$.

مثال ٩ : برهن على أن : π عنصر أولى فى $\mathbb{Z}[i]$ $\Leftarrow$ يوجد عدد أولى $p \in \mathbb{Z}$ بحيث يكون $[\pi] = [p]$ أو $p = \pi\bar{\pi}$.

البرهان : إذا كان π عنصراً أولياً فى $\mathbb{Z}[i]$ فإن : $\pi\bar{\pi} \in \mathbb{N}$ ، $\pi\bar{\pi} > 1$ ($\pi\bar{\pi} = 1$ معناه π وحدة فى $\mathbb{Z}[i]$: تناقض) . ومن ثم ولأن $\mathbb{Z}$ نطاق تحليل وحيد فإنه توجد أعداد أولية

$p_1, ..., p_n \in \mathbb{N}$ بحيث يكون $\pi\bar{\pi} = p_1 ... p_n$. ولأن π عنصر أولى فى $\mathbb{Z}[i]$ فإن π يقسم عاملاً ما p_j ، أى أن $p_j = \pi\alpha$ ، $\alpha \in \mathbb{Z}[i]$.

وهذا يقتضى أن $p_j^2 = p_j\bar{p}_j = (\pi\bar{\pi})(\alpha\bar{\alpha})$. مثلما فى برهان المثال ٨ السابق مباشرة : إما أن يكون $\alpha\bar{\alpha} = 1$ ، أى أن α وحدة فى $\mathbb{Z}[i]$ ، ويكون المثاليان $[p_j]$ ، $[\pi]$ متساويين أى $[p_j] = [\pi]$ ، وإما أن يكون $\alpha\bar{\alpha} = \pi\bar{\pi} = p_j$.

مثال ١٠ : ليكن p عدداً أولياً . برهن على أن :

$$p = 2 \text{ أو } p \equiv 1 \pmod 4 \Rightarrow \exists x \in \mathbb{Z} : x^2 \equiv -1 \pmod p$$

البرهان : إذا كان $p = 2$ خذ $x = -1$.

إذا كان $p \equiv 1 \pmod 4$ فإن :

$$\overline{(p-1)}! = \bar{1} ... \overline{(\frac{p-1}{2})}\overline{(p - \frac{p-1}{2})} ... \overline{(p-1)}$$
$$= \overline{(-1)}^{\frac{p-1}{2}} (\bar{1} ... \overline{(\frac{p-1}{2})}\overline{(\frac{p-1}{2})} ... \bar{1})$$

ضع $x := \bar{1}...(\overline{\frac{p-1}{2}})$. ولأن $\frac{p-1}{2}$ عدد زوجى ينتج مباشرة أن :

$$x^2 \equiv \overline{(p-1)}! \;\equiv\; -1(\bmod p)$$

مثال ١٦ (٢-٢-٨)

<u>مثال ١١</u> : إذا كان n مجموع مربعين فإن :

$$n^2 = a^2 + b^2 : a,b \in \mathbb{Z} \Leftrightarrow n = \alpha\bar{\alpha} : \alpha \in \mathbb{Z}[i]$$

هذا واضح حيث $\alpha = a + ib$ (١)

والآن برهن على أنه إذا كان $n = n_1...n_r$ ، حيث n_i مجموع مربعين ، $i = 1,...,r$ فإن n يكون مجموع مربعين .

<u>البرهان</u> : من (١) $n_i = \alpha\alpha_i$ حيث $\alpha_i \in \mathbb{Z}[i]$ يقتضى أن :

$$n = \alpha_1\bar{a}_1...\alpha_r\overline{\alpha_r} = (\alpha_1...\alpha_r)\overline{(\alpha_1...\alpha_r)} = c^2 + d^2$$

<u>مثال ١٢</u> : ليكن $n > 1$ ، $n \in \mathbb{N}$ ، $n = \prod_p p^{k_p(n)}$ (العدد معبراً عنه بتحليله التحليل الطبيعى إلى عوامله الأولية) .

برهن على أنه إذا كان لجميع الأعداد الأولية $p \equiv 3(\bmod 4)$ يتحقق $k_p(n)$ = عدداً زوجياً فإن n يكون مجموع مربعين أى $n = a^2 + b^2,\ a,b \in \mathbb{Z}$

<u>البرهان</u> : من المثال السابق مباشرة يكفى أن نبرهن على :

(أ) 2 مجموع مربعين

(ب) p عدد أولى ، $p \equiv 1(\bmod 4)$ $\Leftarrow p$ مجموع مربعين

لاحظ أن : $p \equiv 3(\bmod 4)$ عدد أولى $\Leftarrow$ $k_p(n)$ عدد زوجى $\Leftarrow$ $p^{k_p(n)}$ مربع

(أ) $2 = 1^2 + 1^2 = (1+i)(1-i)$

(ب) ليكن $p \equiv 1(\bmod 4)$ عدداً أولياً . من مثال ١٠ السابق يوجد $x \in \mathbb{Z}$ بحيث يكون $x^2 \equiv -1(\bmod p)$ وهذا يقتضى أن $p \mid (x^2 + 1)$ أى أن $p \mid (x+i)(x-i)$. ولكن

من الواضح أن p لايقسم $x+i$ ولايقسم $x-i$ $(\frac{x}{p}\pm\frac{i}{p}\notin\mathbb{Z}[i])$ ، وبالتالى فإن p لايمكن أن يكون عنصراً أولياً فى $\mathbb{Z}[i]$. فمن مثال ٨ السابق يوجد $\pi\in\mathbb{Z}[i]$ بحيث يكون $p=\pi\overline{\pi}$.

نهاية البرهان .

<u>مثال ١٣</u>: ليكن $p\neq 2$ عدداً أوليا . برهن على أن :

$p\in\mathbb{Z}[i]$ عنصر أولى $\Leftrightarrow p\equiv 3(\mathrm{mod}\,4)$

<u>البرهان</u> : "$\Leftarrow$" : فى مثال ١٢ السابق برهنا عملياً على أن :

$p\equiv 1(\mathrm{mod}\,4)\Leftarrow p$ ليس عنصراً أوليا فى $\mathbb{Z}[i]$

$2=(1+i)(1-i)$ ليس عنصراً أوليا فى $\mathbb{Z}[i]$

"$\Rightarrow$" : ليكن p ليس عنصراً أوليا فى $\mathbb{Z}[i]$ هذا يقتضى أنه يوجد عنصر أولى $\pi\in\mathbb{Z}[i]$ بحيث يكون $p=\pi\overline{\pi}$ (مثال ٨ السابق) وهذا يقتضى أن $p=a^2+b^2$ (حيث $a+bi=\pi$ ، $a,b\in\mathbb{Z}$) وهذا يقتضى أن $a^2+b^2\equiv 3(\mathrm{mod}\,4)$ غير ممكن (لجميع $x\in\mathbb{Z}$: $x^2\equiv 0(\mathrm{mod}\,4)$ أو $x^2\equiv 1(\mathrm{mod}\,4)$) .

<u>مثال ١٤</u> : بالرجوع إلى مثال ١٢ السابق برهن على العكس :

n مجموع مربعين أى أن $n=a^2+b^2,\ a,b\in\mathbb{Z}$ يقتضى أنه لجميع الأعداد الأولية $p\equiv 3(\mathrm{mod}\,4)$ تحقق $k_p(n)=2k, k\in\mathbb{N}$

<u>البرهان</u> : ليكن n مجموع مربعين . هذا يستلزم أنه يوجد $\alpha\in\mathbb{Z}[i]$ بحيث يكون $n=\alpha\overline{\alpha}$. ومن حيث إن $\mathbb{Z}[i]$ نطاق تحليل وحيد فإنه يوجد $\pi_1,\ldots,\pi_r\in\mathbb{Z}[i]$ عناصر أولية بحيث يكون :

$$\alpha=\pi_1\ldots\pi_r, n=(\pi_1\overline{\pi}_1)\ldots(\pi_r\overline{\pi}_r).$$

ولكل i ، حيث $1\leq i\leq r$ فإنه من مثال ٩ السابق يكون لدينا حالتان :

الحالة الأولى : توجد وحدة $\gamma_i \in \mathbb{Z}[i]$ بحيث إن $\pi_i = \gamma_i p_i$ حيث p_i عدد أولى فى $\mathbb{Z}$ ، وهذا يستلزم أن :

$$\pi_i \bar{\pi}_i = \gamma_i \bar{\gamma}_i . p_i^2 = p_i^2$$

الحالة الثانية : $\pi_i \bar{\pi}_i$ عدد أولى . وهذا يقتضى من مثال١٣ السابق أن

$$p_i := \pi_i \bar{\pi}_i \equiv 1 (\bmod 4) \quad \text{أو} \quad p_i = 2$$

وهكذا فإننا نحصل فى التحليل الأولى لـــ n على العامل الأولى $p \equiv 3 (\bmod 4)$ فقط على هيئة مربعات .

نهاية البرهان .

مثال ١٥ : برهن على عكس المثال ١٠ .

البرهان : كما فعلنا فى مثال١٢ نبرهن على أن p ليس عنصراً أولياً فى $\mathbb{Z}[i]$ والآن ينتج البرهان مباشرة من مثال١٣ .

مثال ١٦ : برهن على أن $\mathbb{Z}[\sqrt{-6}]$ ليس نطاقاً إقليدياً

البرهان : لاحظ أن

$$\begin{aligned} 10 &= 2.5 \\ &= (2+\sqrt{-6})(2-\sqrt{-6}) \end{aligned}$$

يترك للقارئ البرهنة على أن 2 ، 5 ، $2 \pm \sqrt{-6}$ عناصر غير قابلة للتبسيط فى $\mathbb{Z}[\sqrt{-6}]$. ومن ثم يكون $\mathbb{Z}[\sqrt{-6}]$ ليس نطاق تحليل وحيد ومن (٣-٣-٥) ينتج أن $\mathbb{Z}[\sqrt{-6}]$ ليس نطاقاً إقليدياً .

تمارين

(١) برهن على أن $\mathbb{Z}[\sqrt{5}]$ ليس نطاق تحليل وحيد

(إرشاد : فى $\mathbb{Z}[\sqrt{5}] : (\sqrt{5}-1)(\sqrt{5}+1) = 4 = 2.2$. وبرهن على أن $\sqrt{5}-1$ ، $\sqrt{5}+1$ ، 2 غير قابلة للتبسيط فى $\mathbb{Z}[\sqrt{5}]$) .

(٢) برهن على أن $3X^2+4X+3 \in \mathbb{Z}_5[X]$ تتحلل إلى $(3X+2)(X+4)$ وكذلك إلى $(4X+1)(2X+3)$.

$\mathbb{Z}_5$ حقل وبالتالى يكون $\mathbb{Z}_5[X]$ نطاق مثاليات أساسية (٢-١-١٠) ومن ثم هو نطاق تحليل وحيد (٣-٣-٤) ، فكيف تفسر وجود هذين التحليلين ؟

(٣) برهن على أن $\mathbb{Z}[\sqrt{2}]$ ، $\mathbb{Z}[\sqrt{-2}]$ نطاقا تحليل وحيد .

٣-٤ القاسم المشترك الأعظم والمضاعف المشترك الأصغر

Greatest Common Divisor and Least Common Maltiple

٣-٤-١ تعريف :

ليكن R نطاقا متكاملا . وليكن $a_1,...,a_n \in R$

(أ) يسمى العنصر $d \in R$ **قاسماً مشتركاً** (common divisor) للعناصر a_1 ، ... ، a_n

إذا كان $d \mid a_i$ لجميع $i \in \{1,...,n\}$ ،

ويشار لمجموعة القواسم المشتركة للعناصر a_1 ، ... ، a_n بالرمز $cd(a_1,...,a_n)$.

(ب) يسمى العنصر $m \in R$ **مضاعفاً مشتركاً** (common multiple) للعناصر a_1 ، ... ، a_n إذا كان $a_i \mid m$ لجميع $i \in \{1,...,n\}$

ويشار لمجموعة المضاعفات المشتركة للعناصر a_1 ، ... ، a_n بالرمز $cm(a_1,...,a_n)$.

٣-٤-٢ ملحوظة :

ليكن R نطاقا متكاملا / وليكن $a_1,...,a_n \in R$ ، $e \in R^*$. عندئذ فإن :

(أ) $d \in cd(a_1,...,a_n) \Leftrightarrow [d] \supset [a_1]+...+[a_n]$

([a_i] المثالى المتولد من a_i ، ...)

(ب) $m \in cm(a_1,...,a_n) \Leftrightarrow [m] \subset [a_1] \cap ... \cap [a_n]$

(جـ) $R^* \subset cd(a_1,...,a_n), 0 \in cm(a_1,...,a_n)$

(د) $cd(e,a_1,...,a_n) = R^*$

(هـ) $cm(0,a_1,...,a_n) = \{0\}$

(و) $cd(0,a_1,...,a_n) = cd(a_1,...,a_n)$

(ز) $cm(e,a_1,...,a_n) = cm(a_1,...,a_n)$

(ح) $0 \in cd(a_1,...,a_n) \Leftrightarrow a_1 = ... = a_n = 0$

(ط) $e \in cm(a_1,...,a_n) \Leftrightarrow a_1,...,a_n \in R^*$

<u>البرهان</u> :

(أ) $d \mid a_i$ $\Leftarrow$ يوجد $b \in R$: $db = a_i \Leftarrow a_i \in [d]$

$\Leftarrow [d] \supset [a_1] + ... + [a_n]$

(ب) $a_i \mid m$ $\Leftarrow$ يوجد $b \in R$: $a_i b = m \Leftarrow m \in [a_i]$

$\Leftarrow [m] \subset [a_1] + ... + [a_n]$

يترك باقى الملحوظة كتمرين بسيط للقارئ .

<u>**٣-٤-٣ تعريف**</u> :

يقال لعناصر $a_1,...,a_n \in R$ (R نطاق متكامل) إنه <u>**ليس لها قواسم مشتركة**</u> إذا كان $cd(a_1,...,a_n) \subset R^*$. (من (جـ) فى (٣-٤-٢) ينتج أن $cd(a_1,...,a_n) = R^*$)

<u>**٣-٤-٤ ملحوظة**</u> :

ليكن R نطاقاً متكاملاً ، وليكن p عنصراً غير قابل للتبسيط فى R . عندئذ فإنه لكل $a \in R$ إما أن يكون p قاسماً لـــ a (برموز واضحة $p \mid a$ كما سبق) وإما لايكون لهما قواسم مشتركة .

<u>البرهان</u> : ليكن p ، a لهما قواسم مشتركة . عندئذ فإنه يوجد $d \in R \setminus R^*$ بحيث يكون $d \mid a$ ، $d \mid p$. أى أنه يوجد $a', p' \in R$ بحيث يكون $p = dp'$ ، $a = da'$.
ولأن p غير قابل للتبسيط فإن p' يكون وحدة، وبهذا يكون p ، d متشاركين (associate).
ومن ثم فإن p يكون قاسماً لـــ a .

<u>**٣-٤-٥ تعريف**</u> :

ليكن R نطاقاً متكاملاً . وليكن $a_1,...,a_n \in R$.

(أ) يقال لعنصر $g \in R$ إنه <u>**قاسم مشترك أعظم**</u> (greatest common divisor) لـــ a_1 ، ... ، a_n إذا كان $g \in cd(a_1,...,a_n)$ ، لجميع $d \in cd(a_1,...,a_n)$ فإن $d \mid g$

ويشار إلى مجموعة القواسم المشتركة العظمى للعناصر a_1 ،…، a_n بالرمز $gcd(a_1,...,a_n)$

(ب) يقال لعنصر $\ell \in R$ إنه <u>**مضاعف مشترك أصغر**</u> (least common multiple) عندما يكون $\ell \in cm(a_1,...,a_n)$ ، لجميع $m \in cm(a_1,...,a_n)$ فإن $\ell \mid m$

ويشار لمجموعة المضاعفات المشتركة الصغرى للعناصر a_1 ،…، a_n بالرمز $\ell cm(a_1,...,a_n)$

<u>**٣-٤-٦ مثال**</u> :

بمساعدة المثال (٣-٢-١٠) يمكن للقارئ أن يتأكد أنه لايوجد قاسم مشترك <u>أعظم</u> للعنصرين 9 ، $3(2+i\sqrt{5})$ فى $\mathbb{Z}[\sqrt{-5}]$

<u>**٣-٤-٧ ملحوظة**</u> :

ليكن R نطاقاً متكاملاً ، وليكن $a_1,...,a_n \in R$ عندئذ فإن :

(أ) $g \in gcd(a_1,...,a_n), g \sim g' \Rightarrow g' \in gcd(a_1,...,a_n)$

(ب) $g, g' \in gcd(a_1,...,a_n) \Rightarrow g \sim g'$

(جـ) $\ell \in \ell cm(a_1,...,a_n), \ell \sim \ell' \Rightarrow \ell' \in \ell cm(a_1,...,a_n)$

(د) $\ell, \ell' \in \ell cm(a_1,...,a_n) \Rightarrow \ell \sim \ell'$

<u>**البرهان**</u> : مباشر تماماً من التعريف (٣-٤-٥)

والملحوظة تعنى أن القاسم المشترك الأعظم والمضاعف المشترك الأصغر وحيدان بدون حساب الوحدات (up to units)

<u>**٣-٤-٨ ملحوظة**</u> :

ليكن R نطاقاً متكاملاً . ولتكن $a_1,...,a_n \in R$ ليست جميعاً أصفاراً . عندئذ فإن :

لجميع $i \in \{1,...,n\}$: $g \in gcd(a_1,...,a_n), a_i = ga_i'$

ينتج أن : a_1' ، … ، a_n' ليس بينها قواسم مشتركة .

<u>**البرهان**</u> : المطلوب البرهنة على أن :

$cd(a'_1,...,a'_n) \subset R^*$

ليكن $t \in cd(a'_1,...,a'_n) \subset R^*$. عندئذ فإنه لكل $i \in \{1,...,n\}$ يوجد $t_i \in R$ بحيث إن : $a'_i = tt_i$. ينتج أن : $a_i = (gt)t_i$ لكل $i \in \{1,...,n\}$. ومن ثم فإن : $gt \in cd(a_1,...,a_n)$ بحيث يكون $gt \mid g$. ومن ثم فإنه يوجد $s \in R$ بحيث يكون $g = gts$ ، أى بحيث يكون $ts = 1$ ، بعبارة إخرى t تكون وحدة فى R .

<u>٣-٤-٩ نظرية</u> :

فى أى نطاق تحليل وحيد R يوجد لكل $a_1,...,a_n \in R$ قاسم مشترك أعظم ، مضاعف مشترك أصغر.

<u>البرهان</u> : بسبب (٣-٤-٢) نستطيع بدون أى فقد للعمومية أن نفترض أن $a_1,...,a_n \in R \setminus \{0\}$ ، أن $a_1,...,a_n \notin R^*$ ولأن R نطاق تحليل وحيد فإنه توجد عناصر غير قابلة للتبسيط $p_1,...,p_r \in R$ ولكل $i \in \{1,...,n\}$ توجد أعداد طبيعية : $k_1(a_i)$ ، ... ، $k_r(a_i)$ بحيث يكون $a_i = p_1^{k_1(a_i)}...p_r^{k_r(a_i)}$ لجميع $i \in \{1,...,n\}$. لكل $j \in \{1,...,r\}$ ليكن $m_j := \min\{k_j(a_i) : i \in \{1,...,n\}\}$

وليكن $M_j := \max\{k_j(a_i) : i \in \{1,...,n\}\}$. عندئذ فإن : $g = p_1^{m_1}...p_r^{m_r}$ قاسم مشترك أعظم ، $\ell = p_1^{M_1}...p_r^{M_r}$ مضاعف مشترك أصغر .

<u>٣-٤-١٠ نتيجة</u> :

ليكن R نطاق تحليل وحيد ، وليكن $Q(R)$ حقل القسمة لـــ R . عندئذ فإنه لكل $x \in Q(R)$ يوجد عنصران a ، b ليس بينهما قواسم مشتركة بحيث يكون $x = \frac{a}{b}$.

البرهان : ليكن $x=\frac{a'}{b'}$. من (٣-٤-٩) يوجد قاسم مشترك أعظم g لـ a' ، b' .

نختار $a,b\in R$ بحيث يكون $a'=ga$ ، $b'=gb$ ، فمن (٣-٤-٨) يكون a ، b ليس

بينهما قواسم مشتركة ونحصل على : $x=\frac{a'}{b'}=\frac{ga}{gb}=\frac{a}{b}$.

٣-٤-١١ ملحوظة :

ليكن R نطاق تحليل وحيد ، ولكن $a_1,...,a_n,b\in R$. وليكن g قاسماً مشتركاً أعظم للعناصر a_1 ، ... ، a_n . عندئذ فإن $b\,g$ يكون قاسماً مشتركاً أعظم للعناصر ba_1 ، ... ، ba_n .

البرهان : واضح أن $b\,g$ قاسم مشترك للعناصر ba_1 ، ... ، ba_n .

ليكن t قاسماً مشتركاً لـ ba_1 ، ... ، ba_n . المطلوب أن نبرهن على أن $t\,|\,bg$. في الحالات $a_1=...=a_n=0$ ، $t=0$ ، $t\in R^*$: الإدعاء واضح. إذا لم تحدث حالة من هذه الحالات الثلاث نختار $a'_1,...,a'_n\in R$ بحيث يكون $a_i=ga'_i$ لجميع $i\in\{1,...,n\}$.

لاحظ أن a'_1 ، ... ، a'_n ليس لها قواسم مشتركة وكلها غير قابلة للتبسيط وباستخدام تحليل العناصر إلى عناصر أولية ينتج أن $t\,|\,bg$.

٣-٤-١٢ نظرية :

ليكن R نطاق مثاليات أساسية، ولتكن $a_1,...,a_n\in R$. عندئذ فإنه لكل $g\in gcd(a_1,...,a_n)$ توجد عناصر $x_1,...,x_n\in R$ بحيث إن :

$$g=x_1a_1+...+x_na_n$$

البرهان: لأن R نطاق مثاليات أساسية فإنه يوجد $g'\in R$ بحيث يكون : $[g']=[a_1,...,a_n]$. ينتج أن $g'\,|\,a_1$ ، ... ، $g'\,|\,a_n$. والآن ليكن $g''\,|\,a_1$ ، ... ، $g''\,|\,a_n$. ينتج أنه يوجد $z_1,...,z_n\in R$ بحيث يكون $g''z_1=a_1$ ، ... ، $g''z_n=a_n$.

والآن $[g']=[a_1,...,a_n]$ يستلزم أنه يوجد $w_1,...,w_n\in R$ بحيث إن $a_1w_1+...+a_nw_n=g'$ ،

ومن ثم فإنه يوجد $z_1,...,z_n,w_1,...,w_n \in R$ بحيث إن : $g''z_1w_1+...+g''z_nw_n=g'$

وهذا يقتضى أن $g''|g'$. أى أن g' قاسم مشترك أعظم لـ a_1 ، ... ، a_n . ومن

(٣-٤-٧) نحصل على $g \sim g'$ ، وهكذا فإن : $[g]=[g']=[a_1,...,a_n]$. ومن ثم

فإنه يوجد $x_1,...,x_n \in R$ بحيث إن : $g=x_1a_1+...+x_na_n$.

نهاية البرهان .

<u>ملحوظة</u> : بصياغة أخرى نكتب

$$[g]=[a_1]+[a_2]+...+[a_n]$$

إذا كان وفقط إذا كان

$$g \in gcd(a_1,a_2,...,a_n)$$

<u>٣-٤-١٣ نتيجة</u> :

ليكن R نطاق مثاليات أساسية ، ولتكن $a_1,...,a_n \in R$.

التقريرات الآتية متكافئة :

(١) a_1 ، ... ، a_n ليس لها قواسم مشتركة

(٢) $gcd(a_1,...,a_n)=R^*$

(٣) يوجد $x_1,...,x_n \in R$ بحيث يكون : $x_1a_1+...+x_na_n=1$

(٤) $[a_1,...,a_n]=R$

<u>البرهان</u> :

" (١) $\Leftarrow$ (٢) " a_1 ، ... ، a_n ليس لها قواسم مشتركة $\Leftarrow$ $cd(a_1,...,a_n)=R^*$ $\Leftarrow$

(1) $gcd(a_1,...,a_n) \subset R^*$. والآن لتكن $u \in R^*$ فينتج أن $u \in cd(a_1,...,a_n)$ ،

ولكل $g \in cd(a_1,...,a_n)=R^*$. يحدث أن : $[g]=R=[u]$ ومن ثم فإن $g|u$

وبالتالى فإن : $u \in gcd(a_1,...,a_n)$ أى أن (2) $R^* \subset gcd(a_1,...,a_n)$. من (1) ،

(2) ينتج أن $gcd(a_1,...,a_n)=R^*$

" (٢) ⇐ (٣) " : نظرية (٣-٤-١٢)

" (٣) ⇐ (٤) " : واضح

" (٤) ⇐ (١) " : $[a_1,...,a_n]=R \Leftarrow 1\in[a_1,...,a_n] \Leftarrow$ يوجد $\lambda_n \in R$ ، ... ، λ_1

بحيث إن $1=\lambda_1 a_1+...+\lambda_n a_n$. والآن ليكن $x\,|\,a_1$ ، ... ، $x\,|\,a_n$ فينتج أنه يوجد

$y_1,...,y_n \in R$ بحيث إن : $xy_1=a_1,...,xy_n=a_n$ وبالتالى فإنه يوجد $\lambda_1,...,\lambda_n \in R$ ،

$y_1,...,y_n \in R$ بحيث إن :

$$1=\lambda_1 xy_1+...+\lambda_n xy_n=(\lambda_1 y_1+...+\lambda_n y_n)x \Rightarrow x\in R^*$$

أى أن a_1 ، ... ، a_n ليس لها قواسم مشتركة .

٣-٤-١٤ نتيجة : (تمهيدية إقليدس) Euclid's Lemma

ليكن R نطاق مثاليات أساسية . وليكن $a,b,c\in R$. إذا كان a ، b ليس لهما قواسم مشتركة فإن : $b\,|\,ac \Rightarrow b\,|\,c$

البرهان : a , b ليس لهما قواسم مشتركة $\Leftarrow$ يوجد $x,y\in R$ بحيث إن :

$$b\,|\,c \underset{b|ac}{\Leftarrow} cxa+cyb=c \Leftarrow xa+yb=1$$

٣-٤-١٥ ملحوظة :

فى نطاق إقليدى $(R,\ d)$ يمكن أن نحسب القاسم المشترك الأعظم t لعنصرين $a,b\in R\setminus\{0\}$ فنوجد $x,y\in R$ بحيث يكون $xa+yb=t$ وذلك باستخدام الخوارزمية الإقليدية (The Euclidean algorithm) كالآتى :

إذا كان b قاسماً لـــ a ، فكل شيء واضح ! وإلا فإنه يوجد $r_1\in R\setminus\{0\}$ ، $q_1\in R$ بحيث يكون : $a=q_1 b+r_1$ ، $d(r_1)<d(b)$. إذا كان r_1 قاسماً لـــ b فإنه من الواضح أن يكون r_1 قاسماً مشتركاً أعظم لـــ a ، b . إذا لم يكن الأمر كذلك فإنه يوجد $r_2\in R\setminus\{0\}$ ، $q_2\in R$ بحيث يكون $b=q_2 r_1+r_2$. نستمر فى الإجراء بقسمة r_1 على r_2 وهكذا ... يوجد فى النهاية $n\in\mathbb{N}$ بحيث يكون $r_n\neq 0$ ، $r_{n+1}=0$ ، ويكون

لدينا متوالية $(d(r_n))_{n\in\mathbb{N}\setminus\{0\}}$ من الأعداد الطبيعية بحيث يكون $d(b)>d(r_1)>d(r_2)>\dots$. وبهذا نحصل على النظام :

$$a=q_1b+r_1 \quad , \quad r_1\neq 0, d(r_1)<d(b)$$
$$b=q_2r_1+r_2 \quad , \quad r_2\neq 0, d(r_2)<d(r_1)$$
$$r_1=q_3r_2+r_3 \quad , \quad r_3\neq 0, d(r_3)<d(r_2)$$
$$\vdots \qquad\qquad\qquad \vdots$$
$$r_{n-2}=q_nr_{n-1}+r_n, \quad r_n\neq 0, d(r_n)<d(r_{n-1})$$
$$r_{n-1}=q_{n+1}\mathrm{r_n}$$

العنصر r_n هو قاسم مشترك أعظم لـــ a ، b .

وعندما نقرأ هذا النظام من أسفل إلى أعلى نحصل على المتتابعة $r_n\,|\,r_{n-1}$ ، $r_n\,|\,r_{n-2}$ ، ... ، $r_n\,|\,r_1$ ، $r_n\,|\,b$ ، $r_n\,|\,a$ ، وبهذا يكون r_n قاسماً مشتركاً لـــ a ، b .

وإذا كان t قاسماً مشتركاً لـــ a ، b فإننا بقراءتنا النظام السابق من أعلى إلى أسفل نحصل على المتتابعة $t\,|\,r_1$ ، $t\,|\,r_2$ ، ... ، $t\,|\,r_n$. أى أن r_n هو قاسم مشترك أعظم لـــ a ، b . وللحصول على x ، y عنصرين فى R بحيث يكون $xa+yb=r_n$ نقرأ النظام السابق مرة أخرى من أعلى إلى أسفل ، فنحصل من المعادلة الأولى على r_1 كتركيبة خطية من a ، b ، وهكذا ...

وفى النهاية نحصل على r_n كتركيبة خطية فى a ، b .

<u>**٣-٤-١٦ أمثلة محلولة**</u> :

<u>**مثال ١**</u> : فى حلقة كثيرات الحدود $\mathbb{Z}[X]$ برهن على أن $X+2$ هو قاسم مشترك أعظم لـــ X^2+2X ، $2X+4$.

<u>**البرهان**</u> : واضح أن $(X+2)\,|\,(2X+4)$ ، $(X+2)\,|\,(X^2+2X)$ ، أى أن $X+2$ قاسم مشترك لكلتا كثيرتى الحدود . يتبقى أن نثبت أنه (قاسم مشترك) أعظم .

إذا كان $f \neq 0$ ، $f \in \mathbb{Z}[X]$ بحيث إن $f \mid (X^2+2X)$ ، $f \mid (2X+4)$ ، فإنه يوجد $g \in \mathbb{Z}[X]$ بحيث إن $fg = 2X+4$. ولأن $\mathbb{Z}$ نطاق متكامل وبالتالى $\mathbb{Z}[X]$ نطاق متكامل (ملحوظة (٢-١-٥ (٣))) فإن :

$$\deg(f)+\deg(g)=\deg(fg)=\deg(2X+4)=1$$

ومن ثم فإنه إما أن يكون $\deg(f)=0$ وأما أن يكون $\deg(g)=0$. إذا كان $\deg(f)=0$ فإن $f=a_0 \neq 0$ ، ومن ثم فإن $f \mid (X^2+2X)$ يقتضى أنه يوجد $b_0,b_1,b_2 \in \mathbb{Z}$ بحيث يكون

$$X^2+2X=a_0(b_0+b_1X+b_2X^2),b_2 \neq 0$$

لأن $\deg(X^2+2X)=2$. وهذا يقتضى أن $a_0b_2=1$. وهذا يستلزم أن $a_0 \in \mathbb{Z}$ وحدة أى أن $a_0=1$ أو $a_0=-1$. وفى الحالتين فإن $a_0 \mid (X+2)$. أى أن $f \mid (X+2)$ فى حالة $\deg(f)=1$ ، ليكن $f=a_0+a_1X$ ، $a_1 \neq 0$.

مرة أخرى $f \mid (2X+4)$ يقتضى أنه يوجد $0 \neq c_0 \in \mathbb{Z}$ بحيث يكون $2X+4=c_0(a_0+a_1X)$. وهذا يستلزم أن $a_0c_0=4$ وهذا يستلزم أن $a_0 \neq 0$. والآن $f \mid (X^2+2X)$ يقتضى أنه يوجد $d_0,d_1 \in \mathbb{Z}$ ، $d_1 \neq 0$ بحيث يكون : $X^2+2X=(a_0+a_1X)(d_0+d_1X)$ (لأن $\deg(X^2+2X)=2$) . ومن ثم فإن : $a_0d_0=0 \underset{a_0 \neq 0}{\Rightarrow} d_0=0$.

$\mathbb{Z}$ نطاق متكامل

وعلاوة على هذا فإن $a_1d_1=1$ وهذا يقتضى أن $a_1 \in \mathbb{Z}$ وحدة أى أن $a_1=\pm 1$. وهذا يستلزم أن $d_1=\pm 1$. وأخيراً فإن $a_0d_1=2$ يستلزم أن $a_0=2$ إذا كان $d_1=1$ ، $a_0=-2$ إذا كان $d_1=-1$. وبالتالى فإن $f=X+2$ أو $f=-X-2$ وفى الحالتين يكون f قاسماً لـ $X+2$. أى أن $X+2$ قاسم مشترك أعظم لـ X^2+2X ، $2X+4$.

مثال٢ : فى $\mathbb{Z}$ يوجد قاسمان مشتركان أعظمان لـ 36 ، 48 هما ± 12 لأنه توجد وحدتان فقط فى $\mathbb{Z}$ هما ± 1 .

فى $\mathbb{Q}[X]$ يوجد قاسم مشترك أعظم لكثيرتى الحدود X^2-2X+1 ، X^3-1 هو $X-1$. ولكل $0 \neq \frac{p}{q} \in \mathbb{Q}$ يكون $\frac{p}{q}(X-1)$ قاسماً مشتركاً أعظم لكثيرتى الحدود X^2-2X+1 ، X^3-1 لأن $0 \neq \frac{p}{q} \in \mathbb{Q}$ وحدة .

أما فى $\mathbb{Z}[X]$ فإن كثيرتى الحدود X^2-2X+1 ، X^3-1 لهما قاسمان مشتركان أعظمان فقط هما $\pm(X-1)$ لأنه لا توجد إلا وحدتان فى $\mathbb{Z}[X]$ هما ± 1 .

<u>مثال ٣</u> : استخدم الخوارزمية الإقليدية لإيجاد القاسم المشترك الأعظم لـــ 49349 ، 15,555 فى $\mathbb{Z}$

<u>الحل</u> :

$$49349 = 3 \times 15555 + 2684$$

$$15555 = 5 \times 2684 + 2135$$

$$2684 = 1 \times 2135 + 549$$

$$2135 = 3 \times 549 + 488$$

$$549 = 1 \times 488 + 61$$

$$488 = 8 \times 61 + 0$$

إذن القاسم المشترك الأعظم هو ± 61

<u>مثال ٤</u> : اوجد القاسم المشترك الأعظم لكثيرتى الحدود

$P_1 := 2X^5+7X^4+9X^3+9X^2+7X+2$ ، $P_2 := 2X^4+3X^3+3X^2+3X+1$

فى $\mathbb{Q}[X]$.

<u>الحل</u> :

$$2X^5+7X^4+9X^3+9X^2+7X+2 = (X+2)(2X^4+3X^3+3X^2+3X+1)$$

وبالتالى فإن $X+2$ يكون قاسماً مشتركاً أعظم . ولجميع $0 \neq \frac{p}{q} \in \mathbb{Q}$ يكون

$\frac{p}{q}(X+2)$ كذلك قاسماً مشتركاً أعظم فى $\mathbb{Q}[X]$.

<u>مثال ٥</u> : اوجد قاسماً مشتركاً أعظم لكثيرتى الحدود :

$$P_1 := X^{10} - 3X^9 + 3X^8 - 11X^7 + 11X^6 - 11X^5 + 19X^4 - 13X^3 + 8X^2 - 9X + 3,$$

$$P_2 := X^6 - 3X^5 + 3X^4 - 9X^3 + 5X^2 - 5X + 2$$

فى $\mathbb{Q}[X]$

<u>الحل</u> : سنستخدم الخوارزمية الإقليدية كالآتى :

$$P_1 = (X^4 - 2X)P_2 + (-X^4 - 3X^3 - 3X^2 - 5X + 3)$$

$$P_2 = (-X^2 + 6X - 19)(-X^4 - 3X^3 - 2X^2 - 5X + 3) + (-59X^3 - 118X + 59)$$

$$-X^4 - 3X^3 - 2X^2 - 5X + 3 = \frac{1}{59}(X+3)(-59X^3 - 118X + 59) + 0$$

أى أن $-59X^3 - 118X + 59$ هو قاسم مشترك أعظم لكثيرتى الحدود فى $\mathbb{Q}[X]$

وكذلك $X^3 + 2X - 1$ هو قاسم مشترك أعظم لكثيرتى الحدود فى $\mathbb{Q}[X]$.

<u>مثال ٦</u> : مستخدماً الخوارزمية الإقليدية اوجد قاسماً مشتركاً أعظم للأعداد 231 ، 630 ، 495 فى $\mathbb{Z}$

<u>الحل</u> :

$$630 = 2 \times 231 + 168$$

$$231 = 1 \times 168 + 63$$

$$168 = 2 \times 63 + 42$$

$$63 = 1 \times 42 + 21$$

$$42 = 2 \times 21 + 0$$

أى أن 21 هو قاسم مشترك أعظم لـــ 630 ، 231 فى $\mathbb{Z}$ (1)

$$630 = 1 \times 495 + 135$$

$$495 = 3 \times 135 + 90$$

$$135 = 1 \times 90 + 45$$

$$90 = 2 \times 45 + 0$$

أى أن 45 قاسم مشترك أعظم لـــ 630 ، 495 فى $\mathbb{Z}$ (2)

$$495 = 2 \times 231 + 33$$

$$231 = 7 \times 33$$

أى أن 33 قاسم مشترك أعظم لـــ 495 ، 231 فى $\mathbb{Z}$ (3)

أى نتيجتين من النتائج الثلاث السابقة (1) ، (2) ، (3) تعطينا قاسماً مشتركاً أعظم للأعداد الثلاثة فى $\mathbb{Z}$. أى أننا نأخذ قاسماً مشتركاً أعظم لاثنين من القواسم المشتركة العظمى الثلاثة السابقة فيكون قاسماً مشتركاً أعظم للأعداد الثلاثة المعطاة فى $\mathbb{Z}$. ويكون هذا القاسم المشترك الأعظم هو 3 .

مثال ذلك قاسم مشترك أعظم لـــ 21 ، 45 هو 3 .

وكان يمكننا كذلك أن نأخذ قاسماً مشتركاً أعظم لأى عددين مع الأعداد الثلاثة ثم نأخذ قاسماً مشتركاً أعظم لهذا القاسم المشترك الأعظم مع العدد الثالث فيكون قاسماً مشتركاً أعظم للأعداد الثلاثة .

مثال ذلك قاسم مشترك أعظم لـــ 21 ، 495 هو 3 .

<u>**مثال ٧**</u> : من (٢-١-٦) ، (٢-١-٨) نعلم أن $(\mathbb{Z},d)$ نطاق إقليدى ، حيث

$$d : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$$
$$n \mapsto |n|$$

$$\forall a,b \in \mathbb{Z} \setminus \{0\} \quad \exists q,r \in \mathbb{Z} : \; a = bq + r \qquad (1)$$

$$r = 0 \;\text{ or }\; d(r) < d(b)$$

وليس هناك قيد على " إشارة " r . ولهذا سنجرى المثال ٦ السابق بطريقة مختلفة قليلاً :

$$630 = 3 \times 231 - 63$$

$$231 = 4 \times 63 - 21$$

$$63 = 3 \times 21$$

إذن يوجد القاسم المشترك الأعظم بين 630 ، 231 هو 21 (كما سبق يوجد قاسم مشترك أعظم آخر هو 21-)

$$630 = 2 \times 495 - 360$$

$$495 = 2 \times 360 - 225$$

$$360 = 2 \times 225 - 90$$

$$225 = 3 \times 90 - 45$$

$$90 = 2 \times 45$$

أى أن 45 قاسم مشترك أعظم بين 630 ، 495

$$495 = 3 \times 231 - 198$$

$$231 = 1 \times 198 + 33$$

$$198 = 6 \times 33$$

أى أن 33 قاسم مشترك أعظم بين 495 ، 231 كما سبق .

<u>مثال ٨</u> : عبر عن القواسم المشتركة العظمى الموجبة فى مثال ٦ بدلالة الأعداد المناظرة فى صورة خطية .

<u>الحل</u> : لدينا

$$\begin{aligned} 21 &= 63 - 42 \\ &= 63 - (168 - 2 \times 63) = 3 \times 63 - 168 \\ &= 3(231 - 168) - 168 = 3 \times 231 - 4 \times 168 \\ &= 3 \times 231 - 4\,(630 - 2 \times 231) = \underline{11 \times 231 - 4 \times 630} \end{aligned}$$

$$\begin{aligned} 45 &= 135 - 90 \\ &= 135 - (495 - 3 \times 135) = 4 \times 135 - 495 \\ &= 4(630 - 495) - 495 = 4 \times 630 - 5 \times 495 \end{aligned}$$

$$33 = 495 - 2 \times 231$$

مثال ٩ : برهن على أنه فى نطاق المثاليات الأساسية يكون لكل عنصرين مضاعف مشترك أصغر .

البرهان : ليكن D نطاق مثاليات أساسية ، وليكن $a,b\in D$.

نحن نعلم أن تقاطع مثاليين يكون مثالياً . ومن حيث إن D نطاق مثاليات أساسية فإنه يوجد $\ell\in D$ بحيث إن :

$$[a]\cap[b]=[\ell] \qquad ([x] \text{ هو المثالى المتولد من } x)$$

سنبرهن على أن ℓ يكون مضاعفاً مشتركاً أصغر لـــ a ، b كالآتى :

$$[a]\cap[b]=[\ell]\Rightarrow[\ell]\subset[a],[\ell]\subset[b]\Rightarrow a\mid\ell,b\mid\ell \qquad (1)$$

أى أن ℓ مضاعف مشترك لـــ a ، b .

والأن ليكن m مضاعفاً مشتركاً لـــ a ، b كذلك ، أى أن : $a\mid m$ ، $b\mid m$. هذا يقتضى أن $[m]\subset[a]$ ، $[m]\subset[b]$ وهذا يستلزم أن $[m]\subset[a]\cap[b]=[\ell]$ أى أن (2) $\ell\mid m$ من (1) ، (2) ينتج أن ℓ مضاعف مشترك أصغر لـــ a ، b .

ملحوظة : يمكن بسهولة تعميم النتيجة السابقة ، فإذا كانت $a_1,\dots,a_n\in D$ حيث D نطاق مثاليات أساسية ، فيوجد مضاعف مشترك أصغر ℓ للعناصر a_1 ، ... ، a_n يعطى بـــ

$$[\ell]=\bigcap_{i=1}^{n}[a_i]$$

مثال ١٠ : برهن على أنه فى نطاق المثاليات الأساسية يكون لكل عنصرين قاسم مشترك أعظم

البرهان : ليكن D نطاق المثاليات الأساسية ، وليكن $a,b\in D$. سنكون مجموع المثاليين $[a]$ ، $[b]$ الذى هو مثالى من (١-٢-٩) . ومن حيث إن D نطاق مثاليات أساسية فإنه يوجد $g\in D$ بحيث يكون

$$[a]+[b]=[g]$$

سنبرهن على أن g قاسم مشترك أعظم لـــ a ، b كالآتى :

$$[a]+[b]=[g]\Rightarrow[a]\subset[g]\Rightarrow\exists x\in D:a=xg\Rightarrow g\mid a \qquad (g \text{ يقسم } a)$$

وبالمثل فإن $g \mid b$.

والآن ليكن $c \mid a$ ، $c \mid b$ $\Leftarrow$ $\exists y, z \in D$ بحيث إن $cy = a$ ، $cz = b$

$\Leftarrow$ $[a] \subset [c]$ ، $[b] \subset [c]$ $\Leftarrow$

$$[g] = [a] + [b] \subset [c]$$

أى أنه يوجد $w \in D$ بحيث يكون $g = wc$ أى أن $c \mid g$ ويكون g قاسماً مشتركاً أعظم لـــ a ، b

راجع كذلك الملحوظة فى (٣-٤-١٢) .

<u>مثال ١١</u> : برهن على أن كثيرة الحدود $\bar{2}X + \bar{1} \in (\mathbb{Z}/4\mathbb{Z})[X]$ لها معكوس ضربى فى $(\mathbb{Z}/4\mathbb{Z})[X]$.

<u>البرهان</u> : لاحظ أن : $(\bar{2}X + 1)^2 = \bar{4}X^2 + \bar{4}X + \bar{1} = \bar{1}$

أى أن $\bar{2}X + \bar{1}$ هى معكوس نفسها الضربى فى $(\mathbb{Z}/4\mathbb{Z})[X]$.

<u>مثال ١٢</u> : ليكن R نطاق مثاليات أساسية ، $0 \neq a, b \in R$. برهن على أن :

$[a], [b]$ مثاليين متعاظميين معاً $\Leftrightarrow$ $1 \in gcd(a, b)$

(راجع تعريف المثاليين المتعاظمين معاً فى جبر المثاليات)

<u>البرهان</u> : ليكن d قاسماً مشتركاً أعظم لـــ a ، b . وبالتالى فإنه من الملحوظة فى (٣-٤-١٢) أو من مثال ١٠ السابق يكون $[a] + [b] = [d]$

ولكن $[a]$ ، $[b]$ متعاظمان معاً ، فيكون $[d] = R = [1]$

(وهذا يكون إذا كان وفقط إذا كان $d \in R$ وحدة)

وهذا يكون إذا كان وفقط إذا كان $1 \in gcd(a, b)$

<u>مثال ١٣</u> : برهن أو انف :

(أ) 4 - هو قاسم مشترك أعظم لـــ 12 ، 16 فى $\mathbb{Z}$

(ب) $\frac{1}{5}$ هو قاسم مشترك أعظم لـــ 3 ، 4 فى $\mathbb{Q}$

<u>الحل</u> : (أ) صحيحة $12 \mid 4-$ ، $16 \mid 4-$. ولجميع $x \mid 12$ ، $x \mid 16$ يكون

$$x \in \{\pm 1, \pm 2, \pm 4\}$$

وواضح أن $x \mid -4$

(ب) فى $\mathbb{Q}$: صحيحة $\dfrac{3}{\frac{1}{5}} = 15 \in \mathbb{Q}$ ، $\dfrac{4}{\frac{1}{5}} = 20 \in \mathbb{Q}$

إذا كان $\dfrac{a}{b} \in \mathbb{Q} \setminus \{0\}$ قاسماً لـ 3 ، 4 فإن : $\dfrac{\frac{1}{5}}{\frac{a}{b}} = \dfrac{b}{5a} \in \mathbb{Q}$.

<u>مثال ١٤</u> : برهن على أنه لكل $a, b, n \in \mathbb{Z} \setminus \{0\}$ يكون للمعادلة $ax \equiv b \pmod{n}$ حل فى $\mathbb{Z}$ إذا لم يكن هناك قواسم مشتركة بين a ، n (عدا ± 1)

<u>البرهان</u> : إذا لم يكن هناك قواسم مشتركة بين a ، n (فيما عدا ± 1 بالطبع) كان القاسم المشترك الأعظم الموجب بينهما على الصورة

$$\lambda a + \mu n = 1 \quad , \quad \lambda, \mu \in \mathbb{Z}$$

(انظر (٣-٤-١٢) ، (٣-٤-١٣))

وبالتالى فإن :

$$\lambda ab + \mu nb = b \quad \Rightarrow \quad a(\lambda b) - b = (-\mu b)n$$

وهذا يقتضى أن المعادلة $ax \equiv b \pmod{n}$ لها الحل $x = \lambda b \in \mathbb{Z}$.

<u>مثال ١٥</u> : عمم مثال ١٤ : برهن على أنه لكل $a, b, n \in \mathbb{Z} \setminus \{0\}$ يكون للمعادلة $ax \equiv b \pmod{n}$ حل فى $\mathbb{Z}$ إذا كان وفقط إذا كان القاسم المشترك الأعظم الموجب لـ a ، n يقسم b .

<u>البرهان</u> : إذا كان القاسم المشترك الأعظم الموجب لـ n ، a يقسم b فإننا نكتب

$$\lambda a + \mu n \mid b \quad , \quad \lambda, \mu \in \mathbb{Z}$$

وهذا يقتضى أن $b = \lambda ay + \mu ny$ ، حيث $y \in \mathbb{Z}$

وبوضع $x=\lambda y$ نحصل على : $b=ax+(\mu y)n$ ، أى أن $ax\equiv b(\mathrm{mod}\, n)$

والآن إذا كان القاسم المشترك الأعظم الموجب لـــ a ، n لايقسم b فإنه يكون :

لجميع $\lambda,\mu,\gamma\in\mathbb{Z}$: $\gamma(\lambda a+\mu n)\neq b$

وبالتالى فإنه يكون لجميع $\lambda,\mu\in\mathbb{Z}$: $\lambda a+\mu n\neq b$

ومن ثم فإن المعادلة $ax\equiv b(\mathrm{mod}\, n)$

لايكون لها حل فى $\mathbb{Z}$.

<u>مثال ١٦</u> : بالنظر إلى مثال ١٥ السابق مباشرة وضح بنائية (استدلالية) لتوجد حلا فى $\mathbb{Z}$ للمعادلة $ax\equiv b(\mathrm{mod}\, n)$ حيث $a,b,n\in\mathbb{Z}$

إذا كان للمعادلة حل . استخدم هذه الطريقة لتعيين حل للمعادلة $12x\equiv 18(\mathrm{mod}\, 42)$

<u>الحل</u> : سنوجد " d " القاسم المشترك الأعظم الموجب لـــ a ، n كما جاء فى (٣-٤-١٥)

على الصورة $d=\lambda a+\mu n, \lambda,\mu\in\mathbb{Z}$

إذا لم يكن d قاسماً لـــ b فمن مثال ١٥ السابق مباشرة لايكون للمعادلة $ax\equiv b(\mathrm{mod}\, n)$ حل.

إذا كان d قاسماً لـــ b فلاحظ أن :

$$a\frac{\lambda b}{d}-b=b(\frac{a\lambda-d}{d})=\frac{-b\mu}{d}n$$

ولأن d يقسم b فيكون $\frac{-b\mu}{d}\in\mathbb{Z}$ ويكون للمعادلة

$$ax\equiv b(\mathrm{mod}\, n)$$

حل حيث يعطى " أحد " الحلول x بـــ $x=\frac{\lambda b}{d}$

والآن فى المعادلة $12x\equiv 18(\mathrm{mod}\, 42)$

$$42=(3)\,(12)+6$$
$$12=(2)\,(6)$$

أى أن $(12)(3)-(42)(1)=6$ هو القاسم المشترك الأعظم الموجب لـ 12 ، 42 .

وواضح أنه يقسم 18 . إذن يوجد حل . سنأخذ الحل $x=\dfrac{\lambda b}{d}=\dfrac{(-3)(18)}{6}=-9$.

مرة أخرى لدينا

$$12x=42k+18,\ \ k\in\mathbb{Z}$$

أى أن

$$2x=7k+3,\ \ k\in\mathbb{Z}$$

$$k=-1\Rightarrow x=-2$$
$$k=-3\Rightarrow x=-9$$
$$k=1\Rightarrow x=5$$
$$k=3\Rightarrow x=12$$

وواضح أنه لكل عدد فردى k يوجد حل . وجميع الحلول توضع على الصورة :

$$-9+7\ell,\ \ \ell\in\mathbb{Z}$$

مثال ١٧ : برهن على أن خوارزمية القسمة تسرى فى $\mathbb{Z}[i]$ ، حيث $d(\alpha)=N(\alpha)$ حيث $N(a+ib)=a^2+b^2$ (قارن مع مثال ٧ فى (٣-٢-١١))

البرهان : ليكن $\alpha,\beta\in\mathbb{Z}[i]$ ، $\beta\neq 0$. نكتب $\dfrac{\alpha}{\beta}=r+si,\ \ r,s\in\mathbb{Q}$

نأخذ $q_1,q_2\in\mathbb{Z}$ أقرب ما يمكن إلى العددين الكسريين r , s على الترتيب

ليكن $\sigma=q_1+q_2i$ ، $\rho=\alpha-\sigma\beta$. والآن :

$$\frac{N(\rho)}{N(\beta)}=\frac{N(\alpha-\sigma\beta)}{N(\beta)}=\frac{|\alpha-\sigma\beta|^2}{|\beta|^2}=\left|\frac{\alpha}{\beta}-\sigma\right|^2$$

$$=|r+si-q_1-q_2i|^2=(r-q_1)^2+(s-q_2)^2\le(\frac{1}{2})^2+(\frac{1}{2})^2\le\frac{1}{2}<1$$

مثال ١٨ : ليكن $\alpha=7+2i$ ، $\beta=3-4i$. اوجد σ ، ρ فى $\mathbb{Z}[i]$ بحيث يكون :

$$\alpha=\sigma\beta+\rho\quad,\quad N(\rho)<N(\beta)$$

الحل : مسترشدين بمثال ١٧ السابق مباشرة سنكتب :

$$7+2i=\sigma(3-4i)+\rho \quad , \quad (N(\rho)<3^2+(-4)^2=25$$ بحيث)

$$\frac{7+2i}{3-4i}=\frac{(7+2i)(3+4i)}{(3-4i)(3+4i)}=\frac{13}{25}+\frac{34}{25}i$$

نختار $\sigma=q_1+q_2i=1+i$

لاحظ أن

$$\frac{N(\rho)}{N(\beta)}=|\frac{7+2i}{3-4i}-1-i|^2=|\frac{13}{25}+\frac{34}{25}i-1-i|^2$$
$$=(\frac{-12}{25})^2+(\frac{9}{25})^2=\frac{9}{25}<1$$

وبالتالى فإن

$$7+2i=(1+i)(3-4i)+3i(=\rho)$$

مثال ١٩ : اوجد قاسماً مشتركاً أعظم لـــ $8+6i$ ، $5-15i$ فى $\mathbb{Z}[i]$

الحل : سنتبع نفس الأسلوب كما فى مثال ١٨ المستقى من مثال١٧ السابق . ولهذا سنكتب

$$8+6i=(5-15i)\sigma+\rho,$$

بحيث يكون $N(\rho)<5^2+(-15)^2=250$

$$\frac{\alpha}{\beta}=\frac{8+6i}{5-15i}=\frac{(8+6i)(5+15i)}{(5-15i)(5+15i)}=\frac{-1+3i}{5}$$

إذن نختار $\sigma=q_1+q_2i=0+i$

وتحقق من أن :

$$\frac{N(\rho)}{N(\beta)}=|-\frac{1}{5}+\frac{3i}{5}-i|^2=(-\frac{1}{5})^2+(-\frac{2}{5})^2=\frac{1}{5}<1$$

وبالتالى فإن :

$$8+6i=i(5-15i)+i-7(=\rho)$$

والآن

$$5-15i=(i-7)\sigma'+\rho'$$

$$\frac{5-15i}{i-7}=\frac{(5-15i)}{(i-7)}.\frac{(-i-7)}{(-i-7)}=-1+2i$$

أى أن

$$5-15i=(-1+2i)(i-7)$$

ومن (٣-٤-١٥) يكون القاسم المشترك الأعظم المطلوب هو $i-7$.

تمارين

(١) استخدم الخوارزمية الإقليدية فى $\mathbb{Z}[i]$ لحساب القاسم المشترك الأعظم لـ $16+7i$ ، $10-5i$

(٢) ليكن $[\alpha]$ مثاليا أساسياً فى $\mathbb{Z}[i]$

(أ) برهن على أن $\mathbb{Z}[i]/[\alpha]$ حلقة منتهية

(ب) برهن على أنه إذا كان π عنصراً غير قابل للتبسيط فى $\mathbb{Z}[i]$ فإن $\mathbb{Z}[i]/[\pi]$ يكون حقلاً

(جـ) اوجد عدد عناصر كل من الحقول الآتية :

(أ) $\mathbb{Z}[i]/[3]$ (ب) $\mathbb{Z}[i]/[1+i]$ (جـ) $\mathbb{Z}[i]/[1+2i]$

(إرشاد : انظر مثال ٩ فى (١-٣-٢٠))

(٣) برهن على أن خوارزمية القسمة تسرى فى النطاقات المتكاملة $\mathbb{Z}[\sqrt{-2}]$ ، $\mathbb{Z}[\sqrt{2}]$ ، $\mathbb{Z}[\sqrt{3}]$ ، حيث $d(\alpha)=N(\alpha)$ حيث α عنصر غير صفرى فى أحد هذه النطاقات (وبالتالى فإن هذه النطاقات تكون إقليدية)

٣-٥ حلقات كثيرات الحدود على نطاقات التحليل الوحيد

Polynomial Rings over Unique Factorization Domains

٣-٥-١ تعريف :

ليكن R نطاقاً متكاملاً ، ولتكن $f = \sum_{i=1}^{n} a_i X^i \in R[X] \setminus \{0\}$

(أ) كل قاسم مشترك أعظم لـ a_0 ، ... ، a_n يسمى **محتوى** (content) من f

(ب) يقال إن f **بدائية** (primitive) إذا كان a_0 ، ... ، a_n ليس لها قواسم مشتركة (باستثناء الوحدات)

٣-٥-٢ أمثلة :

(١) {-2, 2} هى مجموعة محتويات كثيرة الحدود $2X^2 + 4X + 8 \in \mathbb{Z}[X]$

(٢) كثيرة الحدود $2X^2 + 4X + 3 \in \mathbb{Z}[X]$ بدائية

٣-٥-٣ ملحوظة :

(١) ليكن R نطاقاً متكاملاً . لكل $f \in R[X] \setminus \{0\}$ ولكل محتوى $I(f)$ من f توجد كثيرة حدود بدائية $f^* \in R[X]$ بحيث إن $f = I(f) f^*$

(٢) إذا كان K حقلاً فإن كل كثيرة حدود $f \in K[X] \setminus \{0\}$ تكون بدائية .

(٣) إذا كان R نطاقاً متكاملاً فإن كل كثيرة حدود غير قابلة للتبسيط (أو غير قابلة للتحليل) $f \in R[X]$ بحيث إن $\deg(f) > 0$ تكون بدائية .

(لاحظ أن كثيرة الحدود $2 \in \mathbb{Z}[X]$ غير قابلة للتبسيط ، لكنها ليست بدائية . ولهذا لايمكن إسقاط الشرط " $\deg(f) > 0$ " .)

(٤) ليكن R نطاق تحليل وحيد ، $Q[R]$ حقل القسمة لـ R . ولتكن $f \in R[X]$ بدائية . عندئذ فإن f غير قابلة للتبسيط فى $Q(R)[X]$ تستلزم أن f غير قابلة للتبسيط فى $R[X]$.

(لاحظ أن كثيرة الحدود $2X + 2 \in \mathbb{Z}[X]$ غير قابلة للتبسيط فى $\mathbb{Q}[X]$ ، لكنها قابلة للتبسيط فى $\mathbb{Z}[X]$ ، ولهذا لايمكن التنازل عن الشرط " f بدائية ").

البرهان : (١) ينتج مباشرة من (٣-٤-٨)

(٢) واضح لأن $K^* = K \setminus \{0\}$

(٣) لتكن f ليست بدائية . عندئذ فإنه يوجد $d \in R \setminus \{0\}$ بحيث إن $d \notin R^*$ ، ويوجد $f' \in R[X]$ بحيث يكون $f = df'$. ولأن $\deg(f') = \deg(f) > 0$ فإن $f' \notin (R[X])^* = R^*$ ، وهذا يقتضى أن f قابلة للتبسيط .

(٤) من $f = gh$ حيث $g,h \in R[X] \subset Q(R)[X]$ ينتج أن $g \in (Q(R))^*$ أو $h \in (Q(R))^*$ وهكذا يكون $g \in R \setminus \{0\}$ أو $h \in R \setminus \{0\}$. وإذا كان $I(f)$ ، $I(h)$ محتوى f ، محتوى h على الترتيب ، فإننا نحصل على $gI(h) \sim I(f) \in R^*$ فى حالة $g \in R \setminus \{0\}$ ، ومن ثم فإن $g \in R^*$. وفى حالة $h \in R \setminus \{0\}$ نحصل بالمثل على $h \in R^*$.

٣-٥-٤ تمهيدية لجاوس Gauss's Lemma

حاصل ضرب كثيرتى حدود بدائيتين هو كثيرة حدود بدائية .

البرهان : لتكن f ، g كثيرتى حدود بدائيتين ، ولتكن fg ليست بدائية . ليكن p قاسم أولى (أى عدد أولى يقسم) محتوى fg ، ولتكن $\bar{f}$ ، $\bar{g}$ ، $\overline{fg}$ كثيرات الحدود التى نحصل عليها من f ، g ، h على الترتيب بعد تخفيض معاملاتها مقياس p . عندئذ فإن $\bar{f}$ ، $\bar{g}$ تنتميان إلى النطاق المتكامل $\mathbb{Z}_p[X]$ ، ويكون $\bar{f}\bar{g} = \overline{fg} = \bar{0}$ حيث $\bar{0}$ هو العنصر الصفرى فى $\mathbb{Z}_p[X]$ (انظر مثال ١٥ فى (٢-٢-٨)) . ولأن $\mathbb{Z}_p[X]$ نطاق متكامل فإنه ينتج أن $\bar{f} = 0$ أو $\bar{g} = 0$. وهذا يعنى أن p يقسم كل معامل فى f أو أن p يقسم كل معامل فى g . أى أن f ليست بدائية أو أن g ليست بدائية . هذا التناقض نهاية البرهان .

ملحوظة : يمكن تعميم التمهيدية ببساطة على أى نطاق تحليل وحيد .

٣-٥-٥ نتيجة :

ليكن R نطاق تحليل وحيد ، وليكن $f, g \in R[X]$. إذا كان $I(f)$ ، $I(g)$ ، $I(fg)$ هى محتويات f، g ، fg على الترتيب فإن :

$$I(fg) \sim I(f)I(g)$$

<u>البرهان</u> : من (٣-٥-٣) توجد كثيرتا حدود بدائيتان $f^*, g^* \in R[X]$ بحيث يكون $f = I(f)f^*$ ، $g = I(g)g^*$. ومن تمهيدية جاوس يتضح أن المحتوى $I(f^*g^*)$ هو وحدة فى R (١) . كذلك لدينا : $fg = I(f)f^*I(g)g^*$ ومنها : $I(fg) \sim I(f)I(g)I(f^*g^*)$ (٢). من (١) ، (٢) ينتج المطلوب مباشرة .

<u>٣-٥-٦ نظرية</u> :

ليكن R نطاق تحليل وحيد ، $f \in R[X] \setminus \{0\}$ ، K هو حقل القسمة لـ R . إذا كان $f = gh$ ، حيث $g, h \in K[X]$ ، فإنه يوجد $a, b \in K^*$ بحيث إن :

(١) $g^* := ag$ ، $h^* := bh$ كثيرتا حدود بدائيتان فى $R[X]$

(٢) $r := \dfrac{1}{ab} \in R$

أى أنه توجد كثيرتا حدود بدائيتان $f^*, g^* \in R[X]$ ، يوجد $r \in R$ بحيث يكون : $f = rg^*h^*$

<u>البرهان</u> : (١) سنبرهن أولاً على أنه لكل كثيرة حدود $0 \neq g = \sum_{i=0}^{n} a_i X^i \in K[X]$ يوجد $a \in K^*$ بحيث يكون $g^* := ag \in R[X]$ بدائية : ليكن $r_i, s_i \in R$ اختيرا بحيث يكون $a_i = \dfrac{r_i}{s_i}$ ، وليكن m هو مضاعف مشترك لـ s_0 ، ... ، s_n . عندئذ فإن $g' := mg$ تقع فى $R[X]$ ، ويوجد محتوى من g' هو $I(g')$ ، وكثيرة حدود بدائية $g^* \in R[X]$ بحيث إن : $g' = I(g')g^*$. ولأن $g \neq 0$ ، $m \neq 0$ فإن $I(g') \neq 0$ ، بحيث نحصل على $g^* = \dfrac{m}{I(g')} g$. ولأن $m \neq 0$ يكون $\dfrac{m}{I(g')} \in K^*$.

(٢) من (١) يوجد $a, b \in K^*$ ، توجد كثيرتا حدود بدائيتان $g^*, h^* \in R[X]$ بحيث إن $f = \dfrac{1}{ab} g^*h^*$. ومن ثم فإنه يوجد $x, y \in R \setminus \{0\}$ بحيث يكون $f = \dfrac{x}{y} g^*h^*$ ونحصل على $yf = xg^*h^*$. وإذا كان $I(f)$ هو محتوى f فإنه من تمهيدية جاوس يوجد

$u \in R^*$ بحيث إن : $yI(f) = xu$ وينتج أن : $\frac{x}{y} = \frac{I(f)}{u} \in R$ أى أننا نحصل فى النهاية على

$$f = \frac{x}{y} g^* h^* = rg^* h^*, r \in R$$

۳-٥-۷ نتيجة هامة :

ليكن R نطاق تحليل وحيد ، $f \in R[X]$ ، K حقل القسمة لـــ R .

f غير قابلة للتبسيط (للتحليل) فى $R[X]$ $\Leftarrow$ f غير قابلة للتبسيط (للتحليل) فى $K[X]$

البرهان : إذا كانت f قابلة للتبسيط فى $K[X]$ فإنه يوجد $g, h \in K[X]$ بحيث إن : $\deg(g) > 0$ ، $\deg(h) > 0$ ، $f = gh$. من (۳-٥-٦) يوجد عندئذ $g^*, h^* \in R[X]$ ، $r \in R$ بحيث إن $\deg(g^*) = \deg(g) > 0$ ، $\deg(h^*) = \deg(h) > 0$ ، $f = rg^* h^*$.

وبالتالى فإن f تكون قابلة للتبسيط فى $R[X]$: تناقض .

۳-٥-۸ نتيجة :

ليكن R نطاق تحليل وحيد، K حقل القسمة لـــ R ، $f \in R[X]$ بدائية ، $g \in R[X] \setminus \{0\}$.

$f | g$ فى $K[X]$ $\Leftarrow$ $f | g$ فى $R[X]$

البرهان : $f | g$ فى $K[X]$ $\Leftarrow$ يوجد $h \in K[X]$ بحيث إن : $g = fh$ $\Leftarrow$ يوجد $f^*, h^* \in R[X]$ ، ويوجد $r \in R$ بحيث إن : $g = rf^* h^*$. ومن برهان (۳-٥-٦) يمكن أن نختار $f^* = \frac{1}{I(f)} f$. ولأن f بدائية يمكن أن نعوض عن f^* بـــ f ونحصل على $g = rfh^*$ ، أى أن $f | g$ فى $R[X]$.

۳-٥-۹ نظرية جاوس :

R نطاق تحليل وحيد $\Leftarrow$ $R[X]$ نطاق تحليل وحيد

البرهان : (١) سنبرهن بالاستقراء الرياضى على درجة كثيرة الحدود أن كل $f \in R[X]$ ، $f \neq 0$ ، $f \notin (R[X])^* = R^*$ يمكن أن تكتب على صورة حاصل ضرب منته من عناصر غير قابلة للتبسيط كالآتى :

كل $f \in R[X]$ ، $f \notin R^*$ ، $\deg(f) = 0$ تقع فى R ، ومن ثم فإنها تكتب على صورة حاصل ضرب منته من عناصر غير قابلة للتبسيط (لأن R نطاق تحليل وحيد)

ليكن $n \in \mathbb{N} \setminus \{0\}$ ، وليكن الادعاء صحيحاً لجميع كثيرات الحدود $h \in R[X]$ ، $h \neq 0$ ، $h \notin R^*$ ، $\deg(h) < n$.

إذا كانت $f \in R[X]$ ، $f \neq 0$ ، $f \notin R^*$ ، $\deg(f) = n$ فإنه يوجد محتوى من f هو $I(f)$ ، كثيرة حدود بدائية $f^* \in R[X]$ بحيث إن : $f = I(f)f^*$.

ولأن R نطاق تحليل وحيد ، $I(f) \in R$ ، فإن $I(f)$ إما أن تكون وحدة أو حاصل ضرب منته من عناصر غير قابلة للتبسيط . وتكون هذه نهاية البرهان إذا كانت f^* غير قابلة للتبسيط . أما إن كانت f^* قابلة للتبسيط فإنه يوجد $g, h \in R[X]$ بحيث إن $f^* = gh$ ، $\deg(g) < \deg(f)^* = n$ ، $\deg(h) < \deg(f)^* = n$.

ومن فرض الاستقراء سنكتب كلاً من g ، h على صورة حاصل ضرب منته من عناصر غير قابلة للتبسيط ، وهكذا تكتب f^* .

(٢) للبرهنة على وحدانية التحليل لتكن c_1 ، ... ، c_m ، p_1 ، ... ، p_n ، d_1 ، ... ، d_k ، q_1 ، ... ، q_ℓ عناصر غير قابلة للتبسيط فى $R[X]$ بحيث إن

$$c_1 .. c_m p_1 ... p_n = d_1 .. d_k q_1 .. q_\ell$$

ولتكن درجات (degrees) c_1 ، ... ، c_m ، d_1 ، ... ، d_k كلها صفراً ، بينما درجات p_1 ، ... ، p_n ، q_1 ، ... ، q_ℓ كلها أكبر من الصفر . من (٣-٥-٣) كل كثيرة حدود درجتها أكبر من الصفر تكون بدائية إذا كانت غير قابلة للتبسيط ومن ثم فإن p_1 ، ... ، p_n ، q_1 ، ... ، q_ℓ كلها بدائية . ومن ثم فإن حاصلى الضرب $p_1 ... p_n$ ، $q_1 ... q_\ell$

بدائيان (تمهيدية جاوس) . ومن ثم فإن : $c_1...c_m \sim d_1...d_k$. ولأن R نطاق تحليل وحيد فإن $m = k$ ، وبترقيم مناسب نستطيع أن نكتب $c_i \sim d_i$ فى R لجميع $i \in \{1,...,m\}$ ومن ثم فإن $p_1...p_n \sim q_1...q_\ell$ فى $K[X]$ (K هو حقل القسمة لـــ R) . ومن (٣-٥-٧) تكون العناصر p_1 ، ... ، p_n ، q_1 ، ... ، q_ℓ غير قابلة للتبسيط فى $K[X]$. ولأن K حقل فإن حلقة كثيرة الحدود $K[X]$ تكون نطاق تحليل وحيد ، ومن ثم فإن $n = \ell$ وبترقيم مناسب نستطيع أن نكتب $p_i \sim q_i$ فى $K[X]$ لجميع $i \in \{1,...,n\}$. وهكذا فإنه ينتج أن : $p_i \mid q_i$ ، $q_i \mid p_i$ فى $K[X]$. ومن (٣-٥-٨) نحصل على $p_i \mid q_i$ ، $q_i \mid p_i$ فى $R[X]$. بحيث إن p_i ، q_i تتشاركان أيضاً فى $R[X]$.

<u>٣-٥-١٠ نتيجة</u> :

R نطاق تحليل وحيد $\Leftarrow$ كل حلقة كثيرات حدود على R فى عدد منته من " العناصر غير المحددة " تكون نطاق تحليل وحيد . وعلى وجه الخصوص إذا كان R حقلاً فإن كل حلقة كثيرات حدود على R فى عدد منته من " العناصر غير المحددة " تكون نطاق تحليل وحيد .

<u>٣-٥-١١ أمثلة محلولة</u> :

<u>مثال١</u> : لتكن $f(X) := a_n X^n + a_{n-1} X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$ ، $a_n \neq 0$. برهن على أنه إذا كان r،s ليس لهما قواسم مشتركة (غير ± 1) ، وكان $f(\frac{r}{s}) = 0$ ، فإن $r \mid a_0$ ، $s \mid a_n$

البرهان : لدينا

$$a_n \frac{r^n}{s^n} + a_{n-1} \frac{r^{n-1}}{s^{n-1}} + ... + a_0 = 0$$
$$\Rightarrow a_n r^n + a_{n-1} s r^{n-1} + ... + a_0 s^n = 0$$
$$\Rightarrow r(a_n r^{n-1} + a_{n-1} s r^{n-2} + ... + a_1 s^{n-1}) = -a_0 s^n$$

r,s ليس لهما قواسم مشتركة (سوى ± 1) فينتج من تمهيدية إقليدس (٣-٤-١٤) أن $r \mid a_0$

وبالمثل $\quad -a_n r^n = s(a_{n-1}r^{n-1} + a_{n-2}sr^{n-2} + \ldots + a_0 s^{n-1})$

ولأن r, s ليس لهما قواسم مشتركة فينتج كما سبق أن $s \mid a_n$.

<u>مثال ٢</u> : اوجد جميع كثيرات الحدود غير القابلة للتبسيط من الدرجة الثانية المطبعة (أى معامل أكبر قوة فيها هو "1") فى $\mathbb{Z}_3[X]$

<u>الحل</u> : ليس هناك سوى $X^2 + \bar{1}$ ، $X^2 + X + \bar{2}$ ، $X^2 + \bar{2}X + \bar{2}$

لاحظ أن $\bar{1} = -\bar{2}$ ، فمثلا $\quad X^2 + X + \bar{1} = X^2 + X - \bar{2} = (X + \bar{2})(X - \bar{1})$

وتكون قابلة للتحليل .

<u>مثال ٣</u> : لتكن $\quad f(X) := X^3 + X^2 + X + 1 \in \mathbb{Z}_2[X]$. اكتب $f(X)$ كحاصل ضرب كثيرات حدود غير قابلة للتبسيط فى $\mathbb{Z}_2[X]$

<u>الحل</u> :

$$\begin{aligned} X^3 + X^2 + X + \bar{1} &= (X^2 + \bar{1})(X + \bar{1}) \\ &= (X^2 - \bar{1})(X + \bar{1}) \\ &= (X - \bar{1})(X + \bar{1})(X + \bar{1}) = (X + \bar{1})(X + \bar{1})(X + \bar{1}) \end{aligned}$$

<u>مثال ٤</u> : لتكن $f(X) \in \mathbb{Z}_p[X]$ ، غير قابلة للتحليل ومن درجة n ، p عدد أولى .

برهن على أن $\mathbb{Z}_p[X]/[f(X)]$ حقل ذو p^n من العناصر

<u>البرهان</u>: $f(X) \in \mathbb{Z}_p[X]$ غير قابلة للتحليل يستلزم أن المثالى $[f(X)]$ مثالى أعظم فى $\mathbb{Z}_p[X]$ (٣-٢-٩) ومن ثم فإن $\mathbb{Z}_p[X]/[f(X)]$ يكون حقلاً (١-٣-١١)

والآن :

$$\mathbb{Z}_p[X]/[f(X)] = \{a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + [f(X)] \mid a_i \in \mathbb{Z}_p, i = 0,1,\ldots,n-1\}$$

ويكون عدد العناصر فى هذا الحقل p^n .

مثال ٥ : لنعتبر $\mathbb{Z}[X]$.

(أ) هل $\mathbb{Z}[X]$ نطاق تحليل وحيد ؟ ولماذا ؟

(ب) برهن على أن $I := \{a + Xf(X) \mid a \in 2\mathbb{Z}, f(X) \in \mathbb{Z}[X]\}$

مثالى فى $\mathbb{Z}[X]$

(جـ) هل $\mathbb{Z}[X]$ نطاق مثاليات أساسية ؟

(د) هل $\mathbb{Z}[X]$ نطاق إقليدى ؟ ولماذا ؟

الحل:

(أ) نعلم من (٣-٣-٦) مثال ١ أن $\mathbb{Z}$ نطاق تحليل وحيد ، وبالتالى فإنه من نظرية جاوس (٣-٥-٩) يكون $\mathbb{Z}[X]$ نطاق تحليل وحيد

(ب) واضح أن $0 \in I$ أى أن $I \neq \phi$

ليكن $a + Xf(X), b + Xf(X) \in I$. هذا يقتضى أن :

$$a + Xf(X) - (b + Xg(X)) = a - b + X(f(X) - g(X)) \in I$$

(لأن $a, b \in 2\mathbb{Z} \Rightarrow a - b \in 2\mathbb{Z}$)

والآن ليكن $g(X) = b_0 + b_1X + \ldots + b_nX^n \in \mathbb{Z}[X]$ ، $a + Xf(X) \in I$

هذا يقتضى أن :

$$\begin{aligned} g(X)(a + Xf(X)) &= (b_0 + b_1X + \ldots + b_nX^n)(a + Xf(X)) \\ &= b_0a + b_1aX + \ldots + b_naX^n + Xg(X)f(X) \\ &= b_0a + X(b_1a + \ldots + b_naX^{n-1} + g(X)f(X)) \in I \end{aligned}$$

(لأن $b_0a \in 2\mathbb{Z}$)

ومن ثم فإن I مثالى فى $\mathbb{Z}[X]$

(جـ) $\mathbb{Z}[X]$ ليس نطاق مثاليات أساسية . المثالى المعطى فى (ب) ليس مثاليا أساسيا فلا يوجد عنصر وحيد $c + Xh(X)$ يولد I .

تعليل آخر : من (٢-١-١٠) لايمكن أن يكون $\mathbb{Z}[X]$ نطاق مثاليات أساسياً ، وإلا كان $\mathbb{Z}$ حقلاً !

(د) $\mathbb{Z}[X]$ لايمكن أن يكون نطاقاً إقليدياً من النتيجة (٣-٣-٥) وإلا كان $\mathbb{Z}[X]$ نطاق مثاليات أساسية .

مثال ٦ : اوجد أصفار $f := X^5 + \bar{3}X^3 + X^2 + \bar{2}X \in \mathbb{Z}_5[X]$ فى $\mathbb{Z}_5$

الحل : واضح أن $X = \bar{0}$ صفر لـــ f . وبالتجربة نجد أن الصفر الثانى الوحيد هو $X = \bar{4}$ وهو غير مكرر .

أى أن كثيرة الحدود f وهى من الدرجة الخامسة لها صفران فقط فى $\mathbb{Z}_5$ هما $\bar{0}$ ، $\bar{4}$.

مثال ٧ : اعتبر

$$f(x,y) := (3x^3 + 2x)y^3 + (x^2 - 6x + 1)y^2 + (x^4 - 2x)y + (x^4 - 3x^2 + 2)$$

كعنصر فى $(\mathbb{Q}[x])[y]$. اكتب $f(x,y)$ كعنصر فى $(\mathbb{Q}[y])[x]$

الحل :

$$f(x,y) = (y+1)x^4 + (3y^3)x^3 + (y^2 - 3)x^2 + (3y^3 - 6y^2 - 2y)x + y^2 + 2 \in (\mathbb{Q}[x])[y]$$

تمارين

(١) ليكن R نطاق تحليل وحيد . برهن على أن قاسماً غير ثابت (nonconstant divisor) لكثيرة حدود بدائية فى $R[X]$ يكون كذلك كثيرة حدود بدائية .

(٢) اعتبر كثيرة الحدود $X^2 - 2 \in \mathbb{Q}[X]$. هل هى قابلة للتحليل ؟ وإذا اعتبرناها فى $\mathbb{R}[X]$ هل تكون قابلة للتحليل ؟ هل يتناقض هذا مع النتيجة (٣-٥-٧) ؟ ولماذا ؟

(٣) برهن على أن $\mathbb{Z}_5[X]$ نطاق تحليل وحيد . والآن اعتبر كثيرة الحدود $X^4 + 3X^2 + 2X + 4 \in \mathbb{Z}_5[X]$ ، وبرهن على أنها يمكن كتابتها على الصورتين الآتيتين :

$(X-1)^3(X+1)$ ، $(X-1)^2(2X-2)(3X+3)$. هل يتناقض هذا مع كون $\mathbb{Z}_5[X]$ نطاق تحليل وحيد ؟ ولماذا ؟

(٤) ليكن R نطاقاً متكاملاً . صف جميع الوحدات فى :

(أ) $R[X]$ (ب) $\mathbb{Z}_{11}[X]$ (جـ) $\mathbb{Z}_6[X]$

(٥) ليكن F حقلاً . برهن على أن جميع كثيرات الحدود ذات الحد الثابت $a_0 = 0$ تكون مثالياً $[X] \in F[X]$

(٦) ليكن F حقلاً ، وليكن $[X]$ المثالى فى $F[X]$ المعرف فى تمرين (٥) السابق مباشرة. برهن على أن $F[X]\big/[X]$ حقل يتشاكل مع F بالطريقتين الآتيتين :

(أ) كل فصل بواقى (Residue class) فى $F[X]\big/[X]$ يتكون بالضبط من عنصر واحد فى F ، يمكن اختياره كممثل للحساب فى $F[X]\big/[X]$

(ب) بعمل هومومورفيزم $\varphi : F[X] \to F$ يكون نواته $[X]$ ، مع تطبيق نظرية الهومومورفيزم (١-٣-٣)

(٧) برهن على أن كثيرة الحدود $f \in \mathbb{Z}[X]$ غير القابلة للتبسيط تكون بدائية .

(٨) لتكن $f := X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$. إذا كان r عدداً كسرياً (نسبياً) وكان $X - r$ يقسم f فبرهن على أن r عدد صحيح .

(٩) أوجد جميع كثيرات الحدود غير القابلة للتبسيط من الدرجة الثانية أو الثالثة فى $\mathbb{Z}_2[X]$ ، $\mathbb{Z}_3[X]$.

٣-٦ تبسيط (تحليل) كثيرات الحدود Factorization of Polynomials

بصفة عامة فإنه ليس من السهل تماماً تحليل أية كثيرة حدود إلى عوامل أو البرهنة على عدم قابليتها للتحليل إلى عوامل درجتها أصغر من درجة كثيرة الحدود . وسنعطى هنا بعض الأدوات المساعدة .

٣-٦-١ شرط عدم القابلية للتحليل لأيزنشتاين(١٨٥٠)

Eisenstein Criterion (1850)

ليكن $f := a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$

إذا كان هناك عدد أولى p بحيث إن $p \nmid a_n$ ، $p \mid a_{n-1}$ ، ... ، $p \mid a_0$ ، $p^2 \nmid a_0$ فإن f تكون غير قابلة للتحليل (للتبسيط) فى $\mathbb{Z}[X]$

البرهان : إذا كانت f قابلة للتحليل فى $\mathbb{Z}[X]$ فإنه يوجد $g, h \in \mathbb{Z}[X]$ بحيث إن $f = gh$ ، $1 \le \deg(g), \deg(h) < n$. ليكن $g = b_r X^r + \ldots + b_0$ ، $h = c_s X^s + \ldots + c_0$.

عندئذ فإنه لأن $p \mid a_0$ ، $p^2 \nmid a_0$ ، $a_0 = bc$ ينتج أن p يقسم واحداً فقط : إما b_0 ، وإما c_0 . لنفترض أن $p \mid b_0$ ، $p \nmid c_0$. أيضاً لأن $p \nmid a_n = b_r c_s$ فإن $p \nmid b_r$. وبالتالى فإنه يوجد عدد صحيح أصغر t بحيث إن $p \nmid \mathrm{b}_t$. والآن اعتبر

$$a_t = b_t c_0 + b_{t-1} c_1 + \ldots + b_0 c_t$$

بالفرض $p \mid a_t$ ، وباختيار t فإن كل حد على اليمين بعد الحد الأول فى المجموع السابق يقبل القسمة على p . وهذا يستلزم أن p يقسم $b_t c_0$. وهذا مستحيل لأن p عدد أولى ، p لايقسم b_t ولا يقسم c_0 .

ملحوظة : يعمم هذا البرهان مباشرة على $f \in R[X]$ حيث R نطاق متكامل .

٣-٦-٢ نتيجة :

ليكن R نطاق تحليل وحيد ، وليكن K حقل القسمة لـــ R . f المعرفة بالشروط فى (٣-٦-١) تكون غير قابلة للتحليل (للتبسيط) فى $K[X]$ (انظر (٣-٥-٧))

<u>٣-٦-٣ مثال</u> : ليكن p عدداً أولياً . عندئذ فإنه لكل $n \in \mathbb{N} \setminus \{0\}$ تكون كثيرة الحدود $X^n - p \in \mathbb{Q}[X]$ غير قابلة للتحليل (للتبسيط) $(p \nmid 1 \ ، \ p \mid p \ ، \ p^2 \nmid p)$

والآن لجميع $n > 1$ يكون $\sqrt[n]{p}$ عدداً غير نسبى (غير كسرى) لأنه لو كان $\sqrt[n]{p}$ عدداً نسبياً أى أن $\sqrt[n]{p} \in \mathbb{Q}$ فإن $X - \sqrt[n]{p} \in \mathbb{Q}[X]$. ولكننا نعلم أنه لو كان $X - \sqrt[n]{p}$ موجوداً فى $\mathbb{Q}[X]$ فإنه يكون أحد عوامل $X^n - p$ أى أن $X^n - p$ تكون قابلة للتبسيط (للتحليل) وهذا غير ممكن .

<u>٣-٦-٤ تعريف</u> :

لتكن R حلقة إبدالية لها عنصر الوحدة . بسبب الخاصة الكونية (العالمية) لحلقات كثيرات الحدود (٢-١-١) : لكل $g \in R[X]$ يوجد بالضبط هومومورفيزم وحيد $\sigma_g : R[X] \to R[X]$ بحيث يكون $\sigma_g(X) = g$ ، $\sigma_g(a) = a$ لجميع $a \in R$. يسمى σ_g **<u>هومومورفيزم التعويض</u>** (subistitution homomorphism) المتعلق بـــ g .

لكل $f \in R[X]$ نحصل على العنصر $f(g) := \sigma_g(f)$ فى $R[X]$ ، بالتعويض عن X بكثيرة الحدود g فى f . هذا التعريف له مايبرره : ليكن

$$f := a_0 + a_1 X + \ldots + a_n X^n \ ، \ a_0, a_1, \ldots, a_n \in R$$

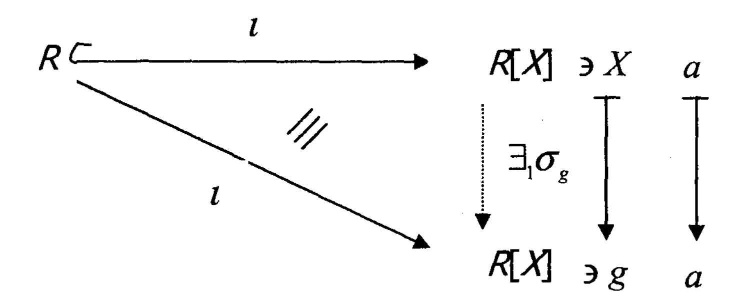
$$\sigma_g(f) = \sigma_g(a_0 + a_1 X + \ldots + a_n X^n) \underset{\sigma_g \text{ هومومورفيزم}}{=} \sigma_g(a_0) + \sigma_g(a_1)\sigma_g(X) + \ldots + \sigma_g(a_n)(\sigma_g(X))^n$$

$$= a_0 + a_1 g + \ldots + a_n g^n = f(g)$$

وعلى وجه الخصوص إذا كان $g = X$ فإننا نحصل على :

$$f = f(X) \qquad \forall f \in R[X]$$

أى أن الكتابتين f ، $f(X)$ متكافئتان .



٣-٦-٥ تمهيدية :

ليكن R نطاقاً متكاملاً ، $g\in R[X]$

هومومورفيزم التعويض σ_g المتعلق بـــ g أيزومورفيزم إذا كان وفقط إذا كان يوجد $a\in R^*$ ، $b\in R$ بحيث إن : $g=aX+b$

البرهان : " $\Rightarrow$ " : ليكن $g=aX+b$ ، $a\in R^*$ ، $b\in R$. لأن $a\in R^*$ فإنه يوجد $a'\in R$ بحيث إن $aa'=1$. نعرف $h:=a'(X-b)$. والآن :

$$(\sigma_g o\sigma_h)(X)=\sigma_g(\sigma_h(X))=\sigma_g(a'(X-b))=aa'(X-b)+b=X\Rightarrow\sigma_g o\sigma_h=1_{R[X]}$$

(راسم الوحدة على $R[X]$)

$$(\sigma_h o\sigma_g)(X)=\sigma_h(\sigma_g(X))=\sigma_h(aX+b)=a'(aX+b-b)=X\Rightarrow\sigma_h o\sigma_g=1_{R[X]}$$

أى أن σ_g تناظر أحادى ، وبالتالى أيزومورفيزم .

" $\Leftarrow$ " : لأن σ_g راسم غامر (شامل ، فوقى) فإنه يوجد $f\in R[X]$ بحيث إن $\sigma_g(f)=X$.

ومن ثم فإن :

$$\deg(g)\deg(f)=\deg(\sigma_g(f))=\deg(X)=1$$

ومن ثم فإن $\deg(g)=1=\deg(f)$. وبالتالى فإنه يوجد $a,b,a',b'\in R$

بحيث إن $g=aX+b,\quad f=a'X+b'$ ، بحيث إن :

$$X=\sigma_g(f)=\sigma_g(a'X+b')=a'(aX+b)+b'=a'aX+a'b+b'$$

$$\Rightarrow aa'=1$$

أى أن $a \in R^*$.

٣-٦-٦ نتيجة :

ليكن R نطاقاً متكاملاً ، $a \in R^*$ ، $b \in R$ ، $g := aX + b$. عندئذ فإنه لكل $f \in R[X]$:

f غير قابلة للتحليل (للتبسيط) فى $R[X] \Leftrightarrow \sigma_g(f)$ غير قابلة للتحليل (للتبسيط) فى $R[X]$

البرهان : مباشر تماماً من التمهيدية السابقة مباشرة (٣-٦-٥)

٣-٦-٧ نتيجة :

لكل p عدد أولى تكون كثيرة الحدود

$$f := X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Q}[X]$$

غير قابلة للتحليل (للتبسيط) (فى $\mathbb{Q}[X]$)

البرهان : ليكن σ_g هو هومومورفيزم التعويض المتعلق بـ $\mathbb{Z}[X] \ni g := X + 1$.

لاحظ أن : $(X-1)f = X^p - 1$ ، ومن ثم فإن

$$\sigma_g((X-1)f) = \sigma_g(X^p - 1)$$

$$\Rightarrow \quad \sigma_g(X-1)\sigma_g(f) = \sigma_g(X^p) - \sigma_g(1)$$

σ_g هومومورفيزم

$$\Rightarrow X\sigma_g(f) = (X+1)^p - 1$$

$$\Rightarrow \sigma_g(f) = X^{p-1} + \binom{p}{1}X^{p-2} + \ldots + \binom{p}{r}X^{p-r-1} + \ldots + \binom{p}{p-1}$$

لكل $r \in \{1, \ldots, p-1\}$ يقع $\binom{p}{r}$ فى $\mathbb{Z}$ ويساوى $\dfrac{p!}{r!(p-r)!}$

ونلاحظ أن $p \mid p!$ ، $p \nmid r!(p-r)!$ (p عدد أولى وإذا كان قاسما لـ $r!(p-r)!$ فلابد أن يقسم أحد العوامل وكلها أصغر من p) ومن ثم فإن :

$p \mid \binom{p}{r}$ لجميع $r \in \{1,\dots,p-1\}$ ، $p \nmid 1$ ، $p \mid \binom{p}{p-1} = p$ ، $p^2 \nmid \binom{p}{p-1}$

ومن (٣-٦-١) تكون $\sigma_g(f)$ غير قابلة للتحليل فى $\mathbb{Z}[X]$ ، ومن (٣-٦-٦) تكون f غير قابلة للتحليل فى $\mathbb{Z}[X]$ ، ومن (٣-٦-٢) تكون f غير قابة للتحليل فى $\mathbb{Q}[X]$.

<u>٣-٦-٨ نظرية</u> (الاختصار بالمقياس)

ليكن R نطاق تحليل وحيد ، $f = \sum_{i=1}^{n} a_i X^i \in R[X]$ كثيرة حدود بدائية ، P مثالى أولى فى R ، $a_n \notin P$. وليكن $\overline{R} := R/P$ ، $\rho : R[X] \to \overline{R}[X]$ امتداداً (extension) للإبيمورفيزم الطبيعى الحلقى $R \to \overline{R}$ ، وليكن K حقل القسمة لـــ R .

عندئذ فإن : $\rho(f) \in \overline{R}[X]$ غير قابل للتحليل $\Leftarrow$ $f \in K[X]$ غير قابل للتحليل

<u>البرهان</u> : من (٣-٥-٧) يكفى أن نبرهن على أن $f \in R[X]$ غير قابلة للتحليل (فى $R[X]$). إذا كانت f قابلة للتحليل فى $R[X]$ فإنه توجد كثيرتا حدود كلتاهما لاتساوى ثابتاً هما g ، h فى $R[X]$ بحيث إن $f = g\,h$ (لأن f بدائية)

ومن ثم فإن $\rho(f) = \rho(g)\rho(h)$. ولأن $\overline{R}$ نطاق متكامل ، $a_n \notin P$ نحصل على :

$$\deg(g) + \deg(h) = \deg(f) \underset{a_n \notin P}{=} \deg(\rho(f)) = \deg(\rho(g)) + \deg(\rho(h))$$

ولأن $\deg(\rho(g)) \le \deg(g)$ ، $\deg(\rho(h)) \le \deg(h)$ فإننا نحصل على

$\deg(\rho(g)) = \deg(g)$ ، $\deg(\rho(h)) = \deg(h)$ ، أى أن $\rho(f)$ تكون قابلة للتحليل فى $\overline{R}[X]$: تناقض

فى حالة $R = \mathbb{Z}$ ، p عدد أولى ، $\overline{R} = \mathbb{Z}/p\mathbb{Z}$. اختيار p يعتمد على شيء من الحظ !

لأنه إذا اتضح أن $\rho(f)$ قابلة للتحليل ، فإن هذا لايعنى شيئاً على الاطلاق ، فقابلية التحليل فى $\overline{R}[X]$ لاتستلزم قابلية التحليل فى $K[X]$.

٣-٦-٩ أمثلة محلولة :

مثال ١ :

لتكن $f := X^5 - X^2 + 1 \in \mathbb{Z}[X]$. نختار $P = 2\mathbb{Z}$ ، وبهذا يكون :

$$\rho(f) = X^5 + X^2 + \bar{1} \in (\mathbb{Z}/2\mathbb{Z})[X]$$

إذا كانت $\rho(f)$ قابلة للتحليل فى $(\mathbb{Z}/2\mathbb{Z})[X]$ فإن $\rho(f)$ يكون لها عامل من الدرجة الأولى أو الدرجة الثانية . كثيرات الحدود من الدرجة الأولى هى X ، $X+\bar{1}$ فقط (فى $(\mathbb{Z}/2\mathbb{Z})[X]$)

X ليس عاملا لـ $\rho(f)$ $\quad \rho(f)(\bar{0}) = \bar{0}+\bar{0}+\bar{1} = \bar{1} \neq \bar{0} \Rightarrow$

$X+\bar{1}$ ليس عاملا لـ $\rho(f)$ $\quad \rho(f)(\bar{1}) = \bar{1}+\bar{1}+\bar{1} = \bar{1} \neq \bar{0} \Rightarrow$

كثيرات الحدود من الدرجة الثانية فى $(\mathbb{Z}/2\mathbb{Z})[X]$ هى :

$$X^2 \text{ ، } X^2+\bar{1} \text{ ، } X^2+X \text{ ، } X^2+X+\bar{1}$$

إذا كان X^2 عاملا من عوامل $\rho(f)$ فإن $\rho(f)(\bar{0}) = \bar{0}$ (لأن ρ هومومورفيزم ، X^2 عامل من عوامل $\rho(f)$) ولكن

X^2 ليس عاملا من عوامل $\rho(f)$ $\quad \rho(f)(\bar{0}) = \bar{0}+\bar{0}+\bar{1} = \bar{1} \neq \bar{0} \Rightarrow$

وإذا كان $X^2+\bar{1}$ عاملا من عوامل $\rho(f)$ فإن $\rho(f)(\bar{1}) = \bar{0}$ ، لكن

$$\rho(f)(\bar{1}) = \bar{1}+\bar{1}+\bar{1} = \bar{1} \neq \bar{0}$$

أى أن $X^2+\bar{1}$ ليس عاملا من عوامل $\rho(f)$

وكذلك إذا كان X^2+X عاملا من عوامل $\rho(f)$ فإن $\rho(f)(\bar{0}) = \rho(f)(\bar{1}) = \bar{0}$ وهذا لايحدث .

يتبقى $X^2+X+\bar{1}$ وبالقسمة الإقليدية نحصل على :

$$\rho(f) = X^5 + X^2 + \bar{1} = (X^3+X^2)(X^2+X+\bar{1}) + \bar{1}$$

أى أن $X^2+X+\bar{1}$ ليس عاملاً من عوامل $\rho(f)$.

وبالتالى فإن $\rho(f)$ ليس لها عوامل من الدرجة الثانية ومن ثم فهى لاتقبل التحليل على الإطلاق فى $(\mathbb{Z}/_{2\mathbb{Z}})[X]$ ومن ثم فهى أى f لاتقبل التحليل فى $\mathbb{Q}[X]$

<u>مثال ٢</u> : برهن على أن شرط عدم القابلية للتحليل لأيزنشتاين ليس ضرورياً (not necessary) . أى أنه شرط كاف (sufficient condition) فقط .

<u>البرهان</u> : لنعتبر $f(X):=X^2+1\in\mathbb{Z}[X]$ عندئذ فإن

$$f(X+1)=(X+1)^2+1=X^2+2X+2$$

خذ $p=2$ ، وطبق شرط أيزنشتاين :

$$2\nmid 1 \text{ ، } 2\mid 2 \text{ ، } 2\mid 2 \text{ ، } 2^2\nmid 2$$

ومن ثم فإن $f(X+1)$ ليست قابلة للتحليل فى $\mathbb{Z}[X]$ ، ومن ثم فهى ليست قابلة للتحليل فى $\mathbb{Q}[X]$.

ومن (٣-٦-٦) تكون $f(X)$ غير قابلة للتحليل فى $\mathbb{Q}[X]$. (هنا $g=X+1$) .

ولكنه لايوجد عدد أولى p يقسم 1 (معامل X^2) . وهذا يبرهن على أن شرط أيزنشتاين ليس ضرورياً.

ملحوظة : يمكن الاستغناء عن النتيجة (٣-٦-٦) هنا بملاحظة أن : $f(X)=g(X)h(X)$ إذا كان وفقط إذا كان $f(X+a)=g(X+a)h(X+a)$ لجميع $a\in\mathbb{Z}$.

وبصفة عامة فإنه إذا كان R نطاق تحليل وحيد ، وكانت $f\in R[X]$ عندئذ فإنه لكل $a\in R$ تكون $f(X)$ غير قابلة للتحليل فى $R[X]$ إذا كان وفقط إذا كان $f(X+a)$ غير قابلة للتحليل فى $R[X]$ ، لأن :

$$f(X)=g(X)h(X)\Leftrightarrow f(X+a)=g(X+a)h(x+a),$$

$$\deg(g(X))=\deg(g(X+a)),\deg(h(X))=\deg(h(X+a))$$

ولهذا فإننا يمكننا أحياناً أن نطبق شرط أيزنشتاين بنجاح عندما نستعيض عن X بـ $X+n$ فى كثيرة الحدود المعنية على $\mathbb{Z}[X]$ ، حيث تكون عادة $n=\pm1,\pm2$.

مثال ٣ : اضرب مثالاً لكثيرة حدود f تكون غير قابلة للتحليل فى $R[X]$ لكنها قابلة للتحليل فى $Q[X]$ حيث Q حقل يحتوى على R .

الحل : فى مثال٢ السابق مباشرة رأينا أن $X^2+1\in\mathbb{Z}[X]$ غير قابلة للتحليل . ولكن $X^2+1=(X+i)(X-i)$ أى أن X^2+1 قابلة للتحليل فى $\mathbb{C}[X]$.

هذا لا يتناقض مع معلوماتنا السابقة فى (٣-٥-٧) ، ذلك أن $\mathbb{C}$ **ليست هى حقل القسمة لـ** $\mathbb{Z}$. ولكن $\mathbb{Q}$ هو حقل القسمة لـ $\mathbb{Z}$.

مثال ٤ : برهن على أن كثيرات الحدود الآتية غير قابلة للتحليل فى $\mathbb{Q}[X]$:

$$7X^4-2X^3+6X^2-10X+18 \quad ، \quad X^3-9X+15 \quad ، \quad X^4-4X+2$$

البرهان : بالنسبة إلى X^4-4X+2 خذ $p=2$ وطبق شرط أيزنشتاين :

$2\nmid 1$ ، $2\mid(-4)$ ، $2\mid 2$ ، $2^2\nmid 2$ إذن كثيرة الحدود غير قابلة للتحليل فى $\mathbb{Z}[X]$ ومن ثم فى $\mathbb{Q}[X]$.

بالنسبة إلى $X^3-9X+15$ ، خذ $p=3$ ، وكما سبق :

$3\nmid 1$ ، $3\mid(-9)$ ، $3\mid 15$ ، $3^2\nmid 15$. إذن $X^3-9X+15$ غير قابلة للتحليل فى $\mathbb{Q}[X]$.

بالنسبة إلى $7X^4-2X^3+6X^2-10X+18$ خذ $p=2$ ، وكما سبق

$2\nmid 7$ ، $2\mid(-2)$ ، $2\mid 6$ ، $2\mid(-10)$ ، $2\mid 18$ ، $2^2\nmid 18$

إذن كثيرة الحدود غير قابلة للتحليل فى $\mathbb{Q}[X]$.

مثال ٥ :

برهن على أن المثالى $[X+2]$ يكون مثالياً أعظم فى $\mathbb{Q}[X]$

البرهان : لأن $\mathbb{Q}$ حقل فمن (٣-٢-٩) إذا كانت $X+2\in\mathbb{Q}[X]$ كثيرة حدود غير قابلة للتحليل (للتبسيط) فإن $[X+2]$ يكون مثالياً أعظم فى $\mathbb{Q}[X]$.

والآن ليكن $X+2=fg$. مرة أخرى لأن $\mathbb{Q}$ حقل فإن $\deg(f)+\deg(g)=1$ (يكفى أن يكون $\mathbb{Q}$ نطاقاً متكاملاً !) . ومن ثم فإنه إما أن تكون $\deg(f)=0$ وإما أن تكون $\deg(g)=0$. إذا كانت $\deg(f)=0$ ، فإن $\deg(g)=1$. ليكن $f=a_0$ ، حيث $0\neq a_0\in\mathbb{Q}$ ، وليكن $g=b_0+b_1X$ حيث $b_0,b_1\in\mathbb{Q}$ ، $b_1\neq 0$. عندئذ فإن : $X+2=a_0(b_0+b_1X)$ ، وهذا يقتضى أن $a_ob_0=2$ ، $a_ob_1=1$. وهكذا فإن a_0 يكون وحدة ، أى أن f وحدة . وبالمثل فإن $\deg(g)=0$ يقتضى أن g وحدة . ومن ثم فإن $X+2$ تكون غير قابلة للتحليل (للتبسيط) فى $\mathbb{Q}[X]$. نهاية البرهان .

<u>ملحوظة</u> : كان من الممكن أن نبرهن على عدم قابلية كثيرة الحدود $X+2\in\mathbb{Q}[X]$ للتحليل مباشرة باستخدام شرط أيزنشتاين ، حيث $p=2$

$2\nmid 1$ ، $2\mid 2$ ، $2^2\nmid 2$

<u>مثال ٦</u> : ليكن F حقلاً . لتكن $f(X)\in F[X]$ ، درجة $f(X)=2$ أو 3 .

عندئذ فإن $f(X)$ قابلة للتحليل على (فى) $F[X]$ إذا كان وفقط إذا كان $f(X)$ لها صفر فى F

<u>البرهان</u> : لتكن $f(X)=g(X)h(X)$ حيث $g(X),h(X)\in F[X]$ ، درجة $(g(X))$ ، درجة $(h(X))$ أقل من درجة $(f(X))$. لأن $F[X]$ نطاق متكامل فإن درجة $(f(X))$ تساوى مجموع درجتى كثيرتى الحدود $g(X)$ ، $h(X)$ ، وهى تساوى 2 أو 3 . ومن ثم فإن واحدة منهما (أى من $g(X)$ ، $h(X)$) على الأقل ستكون درجتها = 1 ، وليكن $g(X)=aX+b$. واضح أن $-a^{-1}b$ صفر لـ $g[X]$ ، وبالتالى هو صفر لـ $f[X]$.

وبالعكس ليكن a صفراً لـ $f(X)$ ، أى أن $f(a)=0$ حيث $a\in F$. عندئذ فمن التمهيدية (٢-٢-٢) يكون $X-a$ عاملاً من عوامل $f(X)$ ، أى أن $f(X)$ قابلة للتحليل فى (على) $F[X]$.

<u>مثال ٧</u> : لأية قيمة لـ $b\in\mathbb{Z}$ تكون كثيرة الحدود $3X^2+bX+5\in\mathbb{Q}[X]$ غير قابلة للتحليل فى $\mathbb{Q}[X]$ ؟

<u>الحل</u>: سنوجد $b\in\mathbb{Z}$ التى تجعل كثيرة الحدود غير قابلة للتحليل فى $\mathbb{Z}[X]$ ، ومن ثم فإنها تكون غير قابلة للتحليل فى $\mathbb{Q}[X]$.

إذا كانت كثيرة الحدود وهى من الدرجة الثانية قابلة للتحليل ، 3 ، 5 ليس بينهما قاسم مشترك غير ± 1 فإنه يكون لها عامل من الدرجة الأولى وبهذا يكون لها صفر فى $\mathbb{Z}$ ، وهذا الصفر يكون على الشكل $\frac{p}{q}$ حيث p أحد عوامل 5 ، q أحد عوامل 3 وبالتجربة نجد أن :

$$\frac{p}{q}=1 \Rightarrow (3)(1)^2+b(1)+5=0 \Rightarrow b=-8$$

$$\frac{p}{q}=-1 \Rightarrow (3)(-1)^2+b(-1)+5=0 \Rightarrow b=8$$

$$\frac{p}{q}=5 \Rightarrow (3)(5)^2+b(5)+5=0 \Rightarrow b=-16$$

$$\frac{p}{q}=-5 \Rightarrow (3)(-5)^2+b(-5)+5=0 \Rightarrow b=16$$

$$\frac{p}{q}=\frac{5}{3} \Rightarrow 3(\frac{5}{3})^2+b(\frac{5}{3})+5=0 \Rightarrow \frac{25}{3}+b(\frac{5}{3})+5=0 \Rightarrow b=-8$$

$$\frac{p}{q}=\frac{-5}{3} \Rightarrow 3(\frac{-5}{3})^2+b(\frac{-5}{3})+5=0 \Rightarrow \frac{25}{3}-b(\frac{5}{3})+5=0 \Rightarrow b=8$$

$$\frac{p}{q}=\frac{1}{3} \Rightarrow 3(\frac{1}{3})^2+b(\frac{1}{3})+5=0 \Rightarrow \frac{1}{3}+b(\frac{1}{3})+5=0 \Rightarrow b=-16$$

$$\frac{p}{q}=\frac{-1}{3} \Rightarrow 3(\frac{-1}{3})^2+b(\frac{-1}{3})+5=0 \Rightarrow \frac{1}{3}-b(\frac{1}{3})+5=0 \Rightarrow b=16$$

إذن لجميع $b\in \mathbb{Z}\setminus\{\pm 8,\pm 16\}$ تكون كثيرة الحدود المعطاة غير قابلة للتحليل فى $\mathbb{Z}[X]$ ، وبالتالى غير قابلة للتحليل فى $\mathbb{Q}[X]$

طريقة أخرى : مميز المعادلة هو :

$$b^2-4(3)(5)=b^2-60$$

$$\Rightarrow X=\frac{-b\pm\sqrt{b^2-60}}{(2)(3)}$$

وحتى يكون هناك حل فى $\mathbb{Z}$ يجب أن يكون $b^2 = 60$ مربعاً وهذا لا يتأتى إلا إذا كان $b = \pm 8$ أو $b = \pm 16$ ، كما سبق .

مثال ٨ : برهن على أن $f := X^3 + X^2 - 2X + 8 \in \mathbb{Q}[X]$ غير قابلة للتبسيط (أى غير قابلة للتبسيط فى $\mathbb{Q}[X]$)

البرهان : سنبرهن على أن كثيرة الحدود المعطاة غير قابلة للتبسيط فى $\mathbb{Z}[X]$ ومن ثم فإنها تكون غير قابلة للتبسيط فى $\mathbb{Q}[X]$ ($\mathbb{Q}$ هو حقل القسمة لــ $\mathbb{Z}$ ، نتيجة (٣-٥-٧))

وكثيرة الحدود المعطاة قواسم معاملاتها المشتركة هى ± 1 فقط فإذا كانت قابلة للتحليل فى $\mathbb{Z}[X]$ فإنه يكون لها عامل من الدرجة الأولى وبهذا يكون لها صفر فى $\mathbb{Z}$. وهذا الصفر هو أحد عوامل 8 ، أى هو أحد ± 1 ، ± 2 ، ± 4 ، ± 8 ($X - a$ عامل من عوامل $f \Leftrightarrow f(a) = 0$)

$$f(1) = (1)^3 + (1)^2 - 2(1) + 8 = 8 \neq 0$$
$$f(-1) = 10 \neq 0, f(2) = 16 \neq 0, f(-2) = 8 \neq 0 .$$
$$f(4) = 80 \neq 0, f(-4) = -32 \neq 0, f(8) = 408 \neq 0, f(-8) = -264 \neq 0$$

وبهذا لايكون لكثيرة الحدود أى صفر فى $\mathbb{Z}[X]$ وبالتالى فهى غير قابلة للتحليل فى $\mathbb{Z}[X]$ ، ومن ثم فى $\mathbb{Q}[X]$.

مثال ٩ : برهن على أن كثيرة الحدود $f := X^5 - 5X^4 - 6X - 1$ غير قابلة للتحليل فى $\mathbb{Q}[X]$.

البرهان : سنثبت – كالمعتاد – أن f غير قابلة للتحليل فى $\mathbb{Z}[X]$ فتكون غير قابلة للتحليل فى $\mathbb{Q}[X]$.

إذا كان لــ f عوامل من الدرجة الأولى فسيكون $f(1) = 0$ أو $f(-1) = 0$ (لأنه لاتوجد عوامل للحد المطلق فى f وهو "1-" سوى ± 1)

$$f(1) = 1 - 5 - 6 - 1 = -11 \neq 0$$
$$f(-1) = -1 - 5 + 6 - 1 = -1 \neq 0$$

إذن ليس لها عوامل من الدرجة الأولى .

بالرجوع إلى النظرية (٣-٦-٨)

نجرب $P = 3\mathbb{Z}$ ، ويكون

$$\rho(f) = X^5 + X^4 + \bar{2}$$

$$\rho(\bar{0}) = \bar{2} \neq \bar{0}, \rho(\bar{1}) = \bar{1} \neq \bar{0}, \rho(\bar{2}) = \bar{2} \neq \bar{0}$$

وليس لـــ $\rho(f)$ عوامل من الدرجة الأولى كما هو متوقع

لأن معامل X^5 هو $\bar{1}$ فإننا نعتبر كثيرات الحدود من الدرجة الثانية التى معامل X^2 فيها هو $\bar{1}$

والآن كثيرات الحدود من الدرجة الثانية فى $(\mathbb{Z}/3\mathbb{Z})[X]$ التى معامل X^2 فيها هو $\bar{1}$ هى :

X^2 ، $X^2+\bar{1}$ ، $X^2+\bar{2}$ ، X^2+X ، $X^2+\bar{2}X$ ، $X^2+X+\bar{1}$ ، $X^2+\bar{2}X+\bar{1}$ ، $X^2+X+\bar{2}$ ، $X^2+\bar{2}X+\bar{2}$

كثيرة الحدود $X^2+\bar{2}X+\bar{1}$ هى $(X+\bar{1})^2$ ، فإذا كان لها صفر هو $\bar{2}$ كان لـــ $\rho(f)$ عامل من الدرجة الأولى ، وهو غير صحيح مما سبق .

إذا كان X^2 أو X^2+X أو $X^2+\bar{2}X$ عاملاً من عوامل $\rho(f)$ كان $\rho(f(\bar{0}))=\bar{0}$ ، ولكن $\rho(f(\bar{0}))=\bar{2}\neq\bar{0}$. إذن X^2 ، X^2+X ، $X^2+\bar{2}X$ لايمكن أن تكون عوامل لـــ $\rho(f(X))$.

إذا كان $X^2+\bar{2}$ أو $X^2+X+\bar{1}$ عاملاً من عوامل $\rho(f)$ كان $\rho(f(\bar{1}))=\bar{0}$ ، ولكن $\rho(f(\bar{1}))=\bar{1}\neq\bar{0}$. إذن $X^2+\bar{2}$ ، $X^2+X+\bar{1}$ لايمكن أن يكونا من عوامل $\rho(f(X))$.

والآن :

$$\rho(f) = (X^3 + X^2 - X - \bar{1})(X^2 + \bar{1}) + X + \bar{3}$$

إذن $X^2+\bar{1}$ ليس عاملاً من عوامل $\rho(f)$

$$\rho(f)=(X^3-\bar{2}X+\bar{2})(X^2+X+\bar{2})+\bar{2}X+\bar{1}$$

إذن $X^2+X+\bar{2}$ ليس عاملاً من عوامل $\rho(f)$

$$\rho(f)=(X^3-X^2+\bar{2})(X^2+\bar{2}X+\bar{2})+\bar{2}X+\bar{1}$$

إذن $X^2+\bar{2}X+\bar{2}$ ليس عاملاً من عوامل $\rho(f)$

أى أن $\rho(f)$ ليس لها عوامل على الإطلاق من الدرجة الثانية وسبق أن ليس لها عوامل من الدرجة الأولى ، أى أن $\rho(f)$ غير قابلة للتحليل فى $(\mathbb{Z}/3\mathbb{Z})[X]$ ، وبالتالى تكون f غير قابلة للتحليل فى $\mathbb{Z}[X]$ ، ومن ثم فى $\mathbb{Q}[X]$.

ملحوظة : كان من الممكن أن نأخذ $P=2\mathbb{Z}$. ونترك هذا للقارىء كتجربة .

مثال ١٠ : المطلوب إنشاء حقل ذى 25 عنصراً

الحل : سنستخدم كثيرة حدود من الدرجة الثالثة f غير قابلة للتحليل فى حقل "مناسب" F فيكون المثالى $[f]$ المتولد منها مثالياً أعظم ، وبالتالى يكون $F[X]/[f]$ حقلاً (نظرية (١-٣-١١)). سنأخذ $\mathbb{Z}/5\mathbb{Z}(=\mathbb{Z}_5)$ حقلاً ونأخذ كثيرة الحدود $X^2+\bar{2}\in\mathbb{Z}_5[X]$ ، وهى غير قابلة للتحليل فى $\mathbb{Z}_5[X]$،

إذ أن :

$$(\bar{0})^2+\bar{2}\neq\bar{0},(\bar{1})^2+\bar{2}=\bar{3}\neq\bar{0},(\bar{2})^2+\bar{2}=\bar{1}\neq\bar{0},(\bar{3})^2+\bar{2}=\bar{1}\neq\bar{0},(\bar{4})^2+\bar{2}=\bar{3}\neq\bar{0}$$

فليس لها أصفار فى $\mathbb{Z}_5$ ، وبالتالى ليس لها عوامل من الدرجة الأولى ، وهى من الدرجة الثانية ، فتكون غير قابلة للتحليل (انظر مثال ٦ السابق)

والآن

$$\mathbb{Z}_5[X]/[X^2+\bar{2}]=\{aX+b+[X^2+\bar{2}]\mid a,b\in\mathbb{Z}_5\}$$

(انظر مثال ١٩ فى (٢-٢-٨))

حقل يتكون من 25 عنصراً لأن كلاً من a ، b يأخذ خمس قيم $\bar{0}$ ، ... ، $\bar{4}$ ، وهما " مستقلان " . (راجع مثال ٤ فى (٣-٥-١١))

مثال١١ : المطلوب إنشاء حقل ذى 27 عنصراً .

الحل : سنأخذ هذه المرة الحقل $\mathbb{Z}/3\mathbb{Z} (=\mathbb{Z}_3)$ ، وسنأخذ كثيرة الحدود $X^3+\bar{2}X+\bar{1}$ وهى كذلك غير قابلة للتحليل فى $\mathbb{Z}_3[X]$ ، لأن :

$$(\bar{0})^3+\bar{2}.\bar{0}+\bar{1}=\bar{1}\neq\bar{0},(\bar{1})^3+\bar{2}.\bar{1}+\bar{1}=\bar{1}\neq\bar{0},(\bar{2})^3+\bar{2}.\bar{2}+\bar{1}=\bar{1}\neq\bar{0}$$

إذن ليس لها أصفار فى $\mathbb{Z}_3[X]$ ، وبهذا لايمكن أن يكون لها عامل من الدرجة الأولى ، وهى من الدرجة الثالثة أى هى غير قابلة للتحليل (انظر مثال٦) . والآن

$$\mathbb{Z}_3[X]\Big/[X^3+\bar{2}X+\bar{1}]=\{aX^2+bX+c+[X^3+\bar{2}X+\bar{1}]\mid a,b,c\in\mathbb{Z}_3\}$$

هو حقل يتكون من 3^3 أى من 27 عنصراً .

ملحوظة : كتدريب حسابى دعنا نحسب :

$$((X^2+\bar{1})+[X^3+\bar{2}X+\bar{1}]).(X^2+X+\bar{1}+[X^3+\bar{2}X+\bar{1}])$$

$$=(X^2+\bar{1})(X^2+X+\bar{1})+[X^3+\bar{2}X+\bar{1}]=X^4+X^3+\bar{2}X^2+X+\bar{1}+[X^3+\bar{2}X+\bar{1}]$$

$$=X(X^3+\bar{2}X+\bar{1})+X^3+\bar{1}+[X^3+\bar{2}X+\bar{1}]$$

$$=X^3+\bar{1}+[X^3+\bar{2}X+\bar{1}]$$ (لأن $X^3+\bar{2}X+\bar{1}\in[X^3+\bar{2}X+\bar{1}]$)

$$=-\bar{2}X+[X^3+\bar{2}X+\bar{1}]=X+[X^2+\bar{2}X+\bar{1}]$$

يمكن كذلك التخلص من X^4 بقسمة X^4 على $X^3+\bar{2}X+\bar{1}$

مثال ١٢ : برهن على أن كثيرة الحدود $X^3+X^2+X+1\in\mathbb{Q}[X]$ تكون قابلة للتحليل (للتبسيط). هل يتناقض هذا مع المثال (٣-٦-٧) ؟

الحل : $X^3+X^2+X+1=(X+1)(X^2+1)$

أى هى قابلة للتحليل . ولا يتناقض هذا مع المثال (٣-٦-٧) لأن هنا $p - 1 = 3$ ، أى $p = 4$ ، 4 ليس عدداً أولياً .

مثال ١٣ : ليكن D نطاقاً متكاملاً ، F حقلاً يحتوى D . إذا كانت $f \in D[X]$ وهى قابلة للتحليل على $D[X]$ ، ولكنها غير قابلة للتحليل على $F[X]$. فبماذا يمكنك القول عن تحليل f على $D[X]$ ؟

الحل : يكون تحليل f فى (على) $D[X]$ على الشكل $f = a\,g$ حيث $a \in D$ ، لكنه ليس وحدة فى D ، $g \in D[X]$.

مثال ١٤ : برهن على أنه لكل عدد صحيح موجب n يوجد عدد لانهائى من كثيرات الحدود فى $\mathbb{Z}[X]$ من الدرجة n ، غير قابلة للتحليل فى $\mathbb{Q}[X]$.

البرهان : لأى عدد أولى p ستكون كثيرة الحدود $f := X^n + p \in \mathbb{Z}[X]$ غير قابلة للتحليل فى $\mathbb{Z}[X]$ (شروط أيزنشتاين متحققة) وبالتالى هى غير قابلة للتحليل فى $\mathbb{Q}[X]$ (نتيجة (٣-٦-٢))

مثال ١٥ : إذا كان p عدداً أولياً فبرهن على أن كثيرة الحدود :

$$f := X^{p-1} - X^{p-2} + X^{p-3} - \ldots - X + 1 \in \mathbb{Q}[X]$$

تكون غير قابلة للتحليل .

البرهان :

انظر مثال (٣-٦-٧) . نأخذ $p \geq 3$. ($p = 2$ الادعاء تافه) .

سنستخدم هومومورفيزم التعويض σ_g المتعلق بـــ $\mathbb{Z}[X] \ni g := X - 1$

لاحظ أن :

$$(X+1)f = X^p + 1$$

$$\Rightarrow \sigma_g((X+1)f) = \sigma_g(X^p + 1)$$

$$\Rightarrow \sigma_g(X+1)\sigma_g(f) = \sigma_g(X^p) + \sigma_g(1)$$

σ_g هومومورفيزم

$$\Rightarrow X\sigma_g(f)=(X-1)^p+1=X^p-\binom{p}{1}X^{p-1}+...+(-1)^r\binom{p}{r}X^{p-r}+...+\binom{p}{p-1}X-1+1$$

$$\Rightarrow \sigma_g(f)=X^{p-1}-\binom{p}{1}X^{p-2}+...+(-1)^r\binom{p}{r}X^{p-r-1}+...+p$$

وأكمل ...

مثال ١٦ : برهن على أن كثيرة الحدود $f:=X^4-2X^2+8X+1\in\mathbb{Q}[X]$ غير قابلة للتحليل فى $\mathbb{Q}[X]$

البرهان : سنبرهن على أن f غير قابلة للتحليل فى $\mathbb{Z}[X]$ ومن ثم تكون غير قابلة للتحليل فى $\mathbb{Q}[X]$ (نتيجة (٣-٥-٧)

لأن " الحد المطلق " هو 1 فلا يوجد سوى ±1 كصفر لكثيرة الحدود إذا أمكن تحليلها وكان أحد عوامل التحليل من الدرجة الأولى . (تذكر أن التحليل فى $\mathbb{Z}[X]$! ، انظر مثال ١ فى (٣-٥-١١) ، تمهيدية (٢-٢-٢)) . ولكن

$$f(1)=1-2+8+1=8\neq0$$
$$f(-1)=1-2-8+1=-8\neq0$$

إذن لايمكن أن تتحل f بحيث يكون أحد عواملها من الدرجة الأولى . أما إن أمكن تحليلها إلى عاملين كل منهما من الدرجة الثانية ($\mathbb{Z}[X]$ نطاق متكامل فيكون مجموع درجتى العاملين = 4 = درجة (f)) فهناك إحدى إمكانيتين للتحليل فقط :

$$f=(X^2+\alpha X+1)(X^2+\beta X+1) \qquad (1)$$

أو

$$f=(X^2+\alpha X-1)(X^2+\beta X-1) \qquad (2)$$

فى (1) لدينا بتسوية المعاملات المتناظرة فى الطرفين :

$0=\alpha+\beta$ (معاملى X^3 فى الطرفين)

$8=\alpha+\beta$ (معاملى X فى الطرفين)

أى أن $8 = 0$ وهذا تناقض

فى (2) لدينا بالمثل بعد تسوية معاملى X^3 ، معاملى X فى الطرفين :

$$0 = \alpha + \beta \ ,$$
$$8 = -\alpha - \beta$$

كذلك $8 = 0$ نفس التناقض السابق

إذن لايمكن تحليل f فى $\mathbb{Z}[X]$ وبالتالى لايمكن تحليلها فى $\mathbb{Q}[X]$.

<u>مثال ١٧</u> :

هل كثيرة الحدود $f := \bar{2}X^3 + X^2 + \bar{2}X + \bar{2}$ غير قابلة للتبسيط فى $\mathbb{Z}_5[X]$ ؟ ولماذا ؟

عبر عن f فى صورة حاصل ضرب كثيرات حدود غير قابلة للتبسيط فى $\mathbb{Z}_5[X]$

<u>الحل</u> : من مثال ٦ السابق لأن f من الدرجة الثالثة فإذا كانت قابلة للتبسيط (للتحليل) فإن أحد عواملها سيكون من الدرجة الأولى. وإذا كان $X - a$ عاملاً من عواملها فإن $f(a)=0$ والعكس (تمهيدية (٢-٢-٢)) وسيكون $\frac{p}{q}$ حيث p ، q أحد عوامل "$\bar{2}$" فى f (مثال ١ من (٣-٥-١١)). والآن عوامل $\bar{2}$ فى f هى $\pm\bar{1}$ ، $\pm\bar{2}$ أو بعبارة أخرى $\bar{1}$ ، $\bar{4}$ ، $\bar{2}$ ، $\bar{3}$ ولكن الأسهل الحساب عند $\pm\bar{1}$ ، $\pm\bar{2}$ كالآتى :

$$f(\bar{1}) = \bar{2} + \bar{1} + \bar{2} + \bar{2} = \bar{2} \neq \bar{0}$$
$$f(-\bar{1}) = -\bar{2} + \bar{1} - \bar{2} + \bar{2} = -\bar{1} = \bar{4} \neq \bar{0}$$
$$f(\bar{2}) = \bar{1} + \bar{4} + \bar{4} + \bar{2} = \bar{1} \neq \bar{0}$$
$$f(-\bar{2}) = -\bar{1} + \bar{4} - \bar{4} + \bar{2} = \bar{1} \neq \bar{0}$$

إذن كثيرة الحدود f غير قابلة للتحليل فى $\mathbb{Z}_5[X]$ (وبالتالى ليست قابلة للتحليل فى $\mathbb{Z}[X]$ وكذلك فى $\mathbb{Q}[X]$ كما سبق) . وبالتالى يكون لدينا حاصل الضرب التافه :

$.\ f = \bar{2}X^3 + X^2 + \bar{2}X + \bar{2}$

مثال ١٨ : ادرس قابلية التحليل لكثيرة الحدود $f := X^3 + \bar{2}X + \bar{2}$ فى $\mathbb{Z}_5[X]$

الحل : تماماً كما فى مثال ١٧ السابق إذا كان هناك تحليل لكثيرة الحدود فسيكون هناك عامل من الدرجة الأولى $X - a$ ، حيث a قاسم لـــ $\bar{2}$ أى أن a هو ± 1 أو ± 2 .
ونحسب $f(a)$ فى كل حالة :

$$f(\bar{1}) = \bar{1} + \bar{2} + \bar{2} = \bar{5} = \bar{0}$$

أى أن $X - \bar{1}$ أحد العوامل

$$f(-\bar{1}) = -\bar{1} - \bar{2} + \bar{2} = -\bar{1} = \bar{4} \neq \bar{0}$$

أى أن $X + \bar{1}$ ليس عاملاً من عوامل f

$$f(\bar{2}) = \bar{3} + \bar{4} + \bar{2} = \bar{4} \neq \bar{0}$$

أى أن $X - \bar{2}$ ليس عاملاً من عوامل f

$$f(-\bar{2}) = -\bar{3} - \bar{4} + \bar{2} = -\bar{5} = \bar{0}$$

أى أن $X + \bar{2}$ عامل من عوامل f
إذن لدينا عاملان من عوامل f وتكون

$$f = h(X - \bar{1})(X + \bar{2})$$

ولأن $\mathbb{Z}_5[X]$ نطاق متكامل فإن

$$\deg(f) = \deg(h) + \deg(X - \bar{1}) + \deg(X + \bar{2}) = \deg(h) + 2 \quad ((\text{انظر } (٢-١-٥)$$

فيكون h من الدرجة الأولى . ولأن المعامل المرشد لـــ $f = 1$ وكذا المعاملان المرشدان فى العاملين $X + \bar{2}$ ، $X - \bar{1}$ فيكون f على الصورة

$$(X + a)(X - \bar{1})(X + \bar{2}) = X^2 + \bar{2}X + \bar{2} (= f)$$

وبتسوية الحدين المطلقين فى الطرفين نحصل على

$$a = -\bar{1}$$

وتكون

$$f = (X - \bar{1})^2 (X + \bar{2})$$
$$(= (X - \bar{1})^2 (X - \bar{3}))$$

<u>مثال ١٩</u> : برهن على أن $f := X^2 + 8X - 2$ غير قابلة للتحليل فى $\mathbb{Q}[X]$ ، لكنها قابلة للتحليل فى $\mathbb{R}[X]$ ، $\mathbb{C}[X]$.

<u>البرهان</u> :إذا كانت f قابلة للتحليل فى $\mathbb{Z}[X]$ فستكون قابلة للتحليل فى $\mathbb{Q}[X]$ ، $\mathbb{R}[X]$ ، $\mathbb{C}[X]$. ونوجد جذور المعادلة $f = 0$ التى هى أصفار كثيرة الحدود f .

$$X^2 + 8X - 2 = 0 \Rightarrow X = \frac{-8 \pm \sqrt{64+8}}{2} = -4 \pm 3\sqrt{2}$$

وبالتالى لاتكون كثيرة الحدود f قابلة للتحليل على $\mathbb{Z}[X]$ أو $\mathbb{Q}[X]$ ، بينما هى قابلة للتحليل على $\mathbb{R}[X]$ ، $\mathbb{C}[X]$.

وليس فى هذا أى تناقض مع النتيجة (٣-٥-٧) لأن حقل القسمة لـ $\mathbb{Q}$ هو $\mathbb{Q}$ نفسه وليس $\mathbb{R}$ أو $\mathbb{C}$.

<u>مثال ٢٠</u> : لتكن $f := 21X^3 - 3X^2 + 2X + 9$. ادرس قابلية f للتحليل فى $\mathbb{Q}[X]$ مستخدماً نظرية الاختصار بالمقياس (٣-٦-٨) .

<u>الحل</u> : سنأخذ $P = 2\mathbb{Z}$ وبهذا يكون لدينا :

$$\bar{f} = X^3 + X^2 + \bar{1}$$

ونعلم أنه إذا كانت f قابلة للتحليل فسيكون لها صفر . ومن حيث إن الحد المطلق $a_0 = \bar{1}$ فإن الصفر المحتمل $\bar{1}$ (انظر مثال ١ فى (٣-٥-١١)) . والآن :

$$(f(\bar{0}) = \bar{1} \neq \bar{0}) \; f(\bar{1}) = \bar{1} \neq \bar{0}$$

إذن كثيرة الحدود غير قابلة للتحليل فى $\mathbb{Z}/_{2\mathbb{Z}}[X]$ وبالتالى فهى غير قابلة للتحليل فى $\mathbb{Q}[X]$.

ملحوظة هامة : إذا اتخذنا $P = 3\mathbb{Z}$ فسيكون لدينا $\bar{f} = \bar{2}X$

وهى غير قابلة للتحليل فى $\mathbb{Z}/3\mathbb{Z}$ لأن $\bar{2}$ وحدة فى $\mathbb{Z}/3\mathbb{Z}$.

لكننا لايمكننا أن نطبق نظرية الاختصار بالمقياس (٣-٦-٨) لأن $a_n = a_3 = \bar{3} \in \mathbb{Z}_3$.

تمارين

(١) ادرس قابلية كثيرة الحدود $f := X^3 + 3X + 2 \in \mathbb{Q}[X]$ للتحليل .

(٢) برهن أو انف :

(أ) $\mathbb{Z}_5[X]/[X^2 + 3X + 2]$ حقل

(ب) $\mathbb{Q}[X]/[X^2 - 2]$ حقل

(٣) أنشئ حقلاً يتكون من تسعة عناصر .

(٤) أنشئ حقلاً يتكون من ثمانية عناصر .

(٥) برهن على أن $X^4 + 1$ غير قابلة للتحليل فى $\mathbb{Q}[X]$ ، لكنها قابلة للتحليل فى $\mathbb{R}[X]$

(٦) برهن على أن $X^4 + X + \bar{4}$ غير قابلة للتحليل فى $(\mathbb{Z}/11\mathbb{Z})[X]$.

(٧) لتكن $f := X^3 + 6$ عنصراً فى $\mathbb{Z}_7[X]$. اكتب f فى صورة حاصل ضرب كثيرات حدود غير قابلة للتبسيط فى $\mathbb{Z}_7[X]$.

(٨) برهن على أن كلاً من $\mathbb{Z}_3[i]$ ، $\mathbb{Z}_3[X]/[X^2 + 1]$ حقل . اسرد عناصر كلا منهما وبرهن على أنهما متشاكلان (انظر مثال٥ فى (١-٣-٢٠))

(٩) اوجد جميع أصفار كثيرة الحدود $f := X^5 + 4X^4 + 4X^3 - X^2 - 4X + 1$

(١٠)) ليكن F حقلاً ، $f \in F[X]$. برهن على أنه لاختبار قابلية التحليل لـــ f يمكننا دائماً أن نتصور أن f مطبعة .

(١١) ليكن F حقلاً ، وليكن $p(X) \in F[X]$ غير قابل للتبسيط . برهن على أن $\{a+[p(X)] \mid a \in F\}$ حقل جزئى من $F[X]/[p(X)]$ ، ويكون متشاكلاً مع F (انظر مثال ٣٤ فى (٢-٢-٨))

(١٢) برهن على أن $f := X^6 + X^5 + X^4 + X^3 + X^2 + X \in \mathbb{Z}[X]$ تتحلل إلى عوامل غير قابلة للتبسيط كالآتى : $X(X+1)(X^2+X+1)(X^2-X+1)$

(١٣) ليكن F حقلاً ، $a \in F \setminus \{0\}$. برهن على أن :

$af(X) \in F[X]$ غير قابلة للتحليل $\Leftarrow$ $f(X) \in F[X]$ غير قابلة للتحليل هل يختلف هذا التمرين عن التمرين (١٠) ؟

(١٤) برهن على أن $f := \frac{3}{7}X^4 - \frac{2}{7}X^2 + \frac{9}{35}X + \frac{3}{5} \in \mathbb{Q}[X]$ غير قابلة للتحليل

(إرشاد : عرف $h := 35f$. f غير قابلة للتحليل فى $\mathbb{Q}[X]$ إذا كان وفقط إذا كان h غير قابلة للتحليل فى $\mathbb{Z}[X]$ ، وأكمل ...)

(١٥) برهن على أن $X^5 + 2X + 4$ غير قابلة للتحليل فى $\mathbb{Q}[X]$

(١٦) حلل $X^4 + \bar{4} \in \mathbb{Z}_5[X]$ إلى عوامل خطية

(١٧) ادرس قابلية تحليل كثيرة الحدود $f := X^3 + \bar{2}X + \bar{3} \in \mathbb{Z}_5[X]$ إلى عوامل غير قابلة للتبسيط. اكتب f كحاصل ضرب كثيرات حدود غير قابلة للتبسيط فى $\mathbb{Z}_5[X]$

(١٨) برهن على أن $f := X^2 + 6X + 12$ غير قابلة للتحليل فى $\mathbb{Q}[X]$. هل هى قابلة للتحليل فى $\mathbb{R}[X]$ ؟ فى $\mathbb{C}[X]$ ؟

(١٩) برهن على أن $X^3 + 3X^2 - 8$ غير قابلة للتحليل فى $\mathbb{Q}[X]$

(٢٠) برهن على أن $X^4 - 22X^2 + 1$ غير قابلة للتحليل فى $\mathbb{Q}[X]$

(٢١) حدد إذا ما كانت التقريرات الآتية صحيحة أم خاطئة :

(أ) $X-2$ غير قابلة للتحليل فى $\mathbb{Q}[X]$

(ب) $3X-6$ غير قابلة للتحليل فى $\mathbb{Q}[X]$

(جـ) X^2-3 غير قابلة للتحليل فى $\mathbb{Q}[X]$

(د) X^2+3 غير قابلة للتحليل فى $\mathbb{Z}_7[X]$

(٢٢) عين أيا من كثيرات الحدود الآتية ، يحقق شرط أيزنشتاين لقابلية التحليل فى $\mathbb{Q}[X]$:

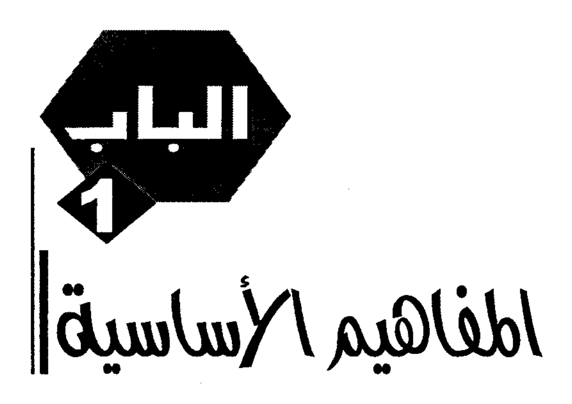
(أ) X^2-12 (ب) $8X^3+6X^2-9X+24$

(جـ) $4X^{10}-9X^3+24X-18$ (د) $2X^{10}-25X^3+10X^2-30$

(٢٣) هل $\mathbb{Q}[X]/[X^2-5X+6]$ حقل ؟ ولماذا ؟ وماذا عن $\mathbb{Q}[X]/[X^2-6X+6]$ ؟

(٢٤) ليكن F حقلاً ، S مجموعة جزئية من $n:F\times F\times\ldots\times F$ من العوامل . برهن على أن مجموعة جميع $f(X_1,\ldots,X_n)\in F[X_1,\ldots,X_n]$ التى تساوى الصفر عند جميع $(a_1,\ldots,a_n)\in S$ تكون مثاليا فى $F[X_1,\ldots,X_n]$.

القسم 3 Field Theory نظرية الحقول



١-١ مميز الحقل The characteristic of a field

١-١-١تعريف : ليكن K حقلا ، "1" عنصر الوحدة فيه . الراسم :

$$\varphi : \mathbb{Z} \to K$$
$$n \mapsto n.1$$

هومومورفيزم حلق لأن :

$$\forall n,m \in \mathbb{Z} : \varphi(n+m) = (n+m).1 = \underbrace{1+\ldots+1}_{n+m \text{ من المرات}} = \underbrace{1+\ldots+1}_{n \text{ من المرات}} + \underbrace{1+\ldots+1}_{m \text{ من المرات}}$$

$$= n.1 + m.1 = \varphi(n) + \varphi(m)$$

بالمثل

$$\varphi(nm) = (nm).1 = (\underbrace{1+\ldots+1}_{n \text{ من المرات}})(\underbrace{1+\ldots+1}_{m \text{ من المرات}}) = (n.1)(m.1)$$

$$= \varphi(n)\varphi(m)$$

(وإذا اعتمدنا الشرط (جـ) فى (١-٢-١) : $\varphi(\underset{\mathbb{Z}}{1}) = \underset{K}{1}.1 = 1$)

من نظرية الحلقات فى مثال ١٨ من (١-٢-٨) نعلم أن نواة هومومورفيزم الحلق يكون مثاليا ، ومن مثال ٣ فى (١-٢-٧) نعلم أن A مثالى فى $\mathbb{Z}$ إذا كان وفقط إذا كان يوجد $m \in \mathbb{N}$ بحيث يكون $A = m\mathbb{Z}$.

إذن يوجد $q \in \mathbb{N}$ بحيث إن $Ker(\varphi) = q\mathbb{Z}$

يقال إن **مميز الحقل K** هو q ، ونكتب $Char(K) := q$

١-١-٢ ملحوظة :

$Char(K)=0 \Leftrightarrow$ φ راسم واحد لواحد $\Leftrightarrow \varphi(n) \neq 0 \quad \forall n \neq 0$

$\Leftrightarrow \quad n.1 \neq 0 \quad \forall n \neq 0$

كذلك فإن

$$Char(K) \neq 0 \quad \Rightarrow \quad \exists n \in \mathbb{N} \setminus \{0\} : n.1 = 0$$

واضح أن هذه الـــ "n" هى أصغر m فى $\mathbb{N} \setminus \{0\}$ بحيث يكون $m.1 = 0$ أى أن المميز فى هذه الحالة هو أصغر m فى $\mathbb{N} \setminus \{0\}$ بحيث يكون $m.1 = 0$.

<u>١-١-٣ أمثلة</u> :

(١) الحقول $\mathbb{Q}$ ، $\mathbb{R}$ ، $\mathbb{C}$ لها المميز 0

(٢) لكل p عدد أولى نعلم أن $\mathbb{Z}/p\mathbb{Z}$ حقل (انظر (١-٣-١٢) فى نظرية الحلقات) ومميزه هو p .

(٣) حقل القسمة لحلقة كثيرات الحدود $(\mathbb{Z}/2\mathbb{Z})[X]$ له المميز "2" ، لكنه يحتوى بالطبع على عدد غير منته من العناصر .

<u>١-١-٤ تعريف</u> :

ذكرنا فى مثال ٣٤ من (٢-٢-٨) تعريف **<u>الحقل الجزئى</u>** (The subfield) k من الحقل K . يسمى K فى هذه الحالة **<u>حقلاً فوقياً</u>** (superfield) للحقل k .

<u>١-١-٥ ملحوظة</u> :

لتكن k مجموعة جزئية من الحقل K . k **<u>حقل جزئى</u>** من K إذا كان وفقط إذا كان :

(١) k يحتوى عنصرين على الأقل .

(٢) لكل $a,b \in k$: $a-b \in k$

(٣) لكل $a,b \in k$ ، $b \neq 0$: $ab^{-1} \in k$

العنصران فى (١) هما "0" صفر زمرة الجمع $(k, +)$ ، "1" عنصر الوحدة فى زمرة الضرب $(k \setminus \{0\}, .)$. (٢) تضمن أن $(k, +)$ زمرة ، (٣) تضمن أن $(k \setminus \{0\}, .)$ زمرة

١-١-٦ ملحوظة :

ليكن k حقلاً جزئياً من الحقل K . لأن عنصر الوحدة فى K هو كذلك عنصر الوحدة فى k فإن $Char(k) = Char(K)$

١-١-٧ ملحوظة :

مميز **الحقل** يساوى الصفر أو هو عدد أولى

البرهان : ليكن K حقلاً ، $Char(K) \neq 0$ ، كذلك المميز ليس عدداً أولياً ، وهكذا فإنه يوجد $m, n \in \mathbb{N}$ بحيث يكون $Char(K) = mn$. وبالتالى فإن

$$0 = (Char(K)).1 = (mn).1 = (m.1)(n.1)$$

ولأن K حقل إذن $m.1 = 0$ أو $n.1 = 0$. ومن ثم فإن $Char(K) \leq m$ أو $Char(K) \leq n$ ، ولأن $Char(K) = mn$ فإنه ينتج أن $m = 1$ أو $n = 1$ ، أى أن $Char(K)$ عدد أولى .

ملحوظة : مميز النطاق المتكامل كذلك يساوى الصفر أو هو عدد أولى

١-١-٨ تعريف :

يقال لحقل P إنه **حقل أولى** (prime field) عندما لايوجد حقل جزئى Q داخله بحيث إن $P \neq Q$.

لكل حقل K يوجد

$$P := \cap\{k \mid k \subset K \quad \text{حقل جزئى} \}$$

وهو حقل أولى بداهة ، ويسمى **الحقل الأولى لـــ K** (The prime field of K)

١-١-٩ نظرية :

ليكن K حقلاً ، P حقله الأولى . عندئذ فإن :

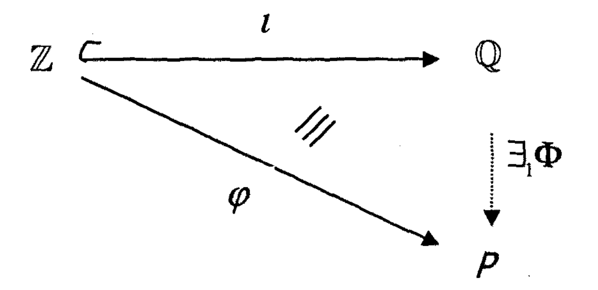
(١) $$Char(K) = 0 \iff P \cong \mathbb{Q}$$

(٢) $$Char(K) = p \neq 0 \iff P \cong \mathbb{Z}/p\mathbb{Z}$$

وهكذا فإنه بدون حساب الأيزومورفيزمات (up to isomorphism) يكون $\mathbb{Q}$ ، $\mathbb{Z}/p\mathbb{Z}$ حيث p عدد أولى الحقلين الأوليين الوحيدين .

<u>**البرهان**</u> : "$\Leftarrow$" فى الحالتين واضح من (١-١-٦)

"$\Rightarrow$" : فى حالة $Char(K)=0$ يكون الراسم $\begin{matrix}\varphi:\mathbb{Z}\to P\\ n\mapsto n.1\end{matrix}$ مونومورفيزم . وبسبب الخاصة الكونية (العالمية) لحقول القسمة يوجد مونومورفيزم $\Phi:\mathbb{Q}\to P$ بحيث يكون $\Phi|\mathbb{Z}=\varphi$. ولأن $\Phi(\mathbb{Q})$ حقل جزئى من الحقل الأولى P ينتج أن $\Phi(\mathbb{Q})=P$ ، ويكون P ، $\mathbb{Q}$ متشاكلين (لأن Φ مونومورفيزم)



فى حالة $Char(K)=p\neq 0$ لدينا $Ker(\varphi)=p\mathbb{Z}$ وبتطبيق نظرية الهومومورفيزم للحلقات (١-٣-٣) ينتج أن

$$\varphi(\mathbb{Z})\cong \mathbb{Z}/Ker(\varphi)=\mathbb{Z}/p\mathbb{Z}$$

ولأن p عدد أولى فإن $\mathbb{Z}/p\mathbb{Z}$ حقل ، وهو حقل جزئى من P ، الذى هو حقل أولى فينتج أن

$$P\cong \mathbb{Z}/p\mathbb{Z}$$

١-١-١٠ أمثلة محلولة :

مثال ١: قرر إذا ما كانت العبارات الآتية صحيحة أو خاطئة

(أ) مميز $n\mathbb{Z}$ هو n

(ب) كل نطاق متكامل مميزه هو الصفر يكون غير منته

(جـ) $\mathbb{Z}$ حقل جزئى من $\mathbb{Q}$

الحل :

(أ) خاطئة ، مميز $n\mathbb{Z}$ هو مميز $\mathbb{Z}$ أى هو الصفر

(ب) صحيحة

(جـ) خاطئة ، $\mathbb{Z}$ ليس حقلاً فلا يوجد معكوس ضربى لـ 2 مثلاً

مثال ٢: اوجد مميز كل من الحلقات الآتية :

(أ) $2\mathbb{Z}$ (ب) $\mathbb{Z}\otimes\mathbb{Z}$

(جـ) $\mathbb{Z}_3\otimes 3\mathbb{Z}$ (د) $\mathbb{Z}_3\otimes\mathbb{Z}_3$

(هـ) $\mathbb{Z}_3\otimes\mathbb{Z}_4$ (و) $\mathbb{Z}_6\otimes\mathbb{Z}_{15}$

(ز) $\mathbb{Z}_4\otimes 4\mathbb{Z}$

الحـل :

(أ) صفر (ب) صفر

(جـ) صفر (د) 3

(هـ) 12 (و) 30

(ز) صفر

سؤال : 12 ، 30 ليسا عددين أوليين هل يتناقض هذا مع (١-١-٧) ؟

مثال ٣ : ليكن R نطاقاً متكاملاً فيه $20.1 = 0$ ، $12.1 = 0$ (تذكر أن $n.1$ معناها المجموع $1+1+...+1$ لـ n من الحدود) . ما مميز R ؟

الحل : من (١-١-٢) نعلم أن المميز إذا كان يساوى الصفر فمعنى هذا أن $n.1 \neq 0$ لجميع $n \in \mathbb{N} \setminus \{0\}$. وهذه ليست الحال هنا

أما إذا كان المميز لا يساوى الصفر فهو أصغر $m \in \mathbb{N} \setminus \{0\}$ بحيث يكون $m.1 = 0$ ، وهو عدد أولى . وبالتالى يكون المميز هنا هو 2 .

مثال ٤ : فى حلقة إبدالية R مميزها هو 2 . برهن على أن العناصر متماثلة القوة تكون حلقة جزئية منها . (راجع مثال ١٠ فى (١-١-١٤) فى نظرية الحلقات) .

البرهان : $0 = 0^2$ وبالتالى 0 عنصر متماثل القوة (١)

ليكن a,b عنصرين متماثلى القوة ، أى أن : $a^2 = a$ ، $b^2 = b$

ينتج أن :

$$(a-b)^2 = a^2 - 2ab + b^2 = a^2 - b^2 = a - b$$

R إبدالية   المميز $= 2$

أى أن $a-b$ متماثل القوة (٢)

$$(ab)^2 = abab = aabb = a^2b^2 = ab$$

R إبدالية

إذن ab متماثل القوة (٣)

من (١) ، (٢) ، (٣) ينتج المطلوب مباشرة .

مثال ٥ : اوجد أصغر حقل جزئى من حقل الأعداد الحقيقة يحتوى على $\sqrt{2}$

الحل : الحقل الجزئى المطلوب هو

$$\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$$

انظر مثال ٢١ فى (١-١-١٥) من نظرية الحلقات

وواضح أنه أصغر حقل جزئى من $\mathbb{R}$ يحتوى على $\sqrt{2}$ ، لأن أى حقل جزئى من $\mathbb{R}$ يحتوى على $\sqrt{2}$ لابد أن يحتوى على $a + b\sqrt{2}$ حيث $a,b \in \mathbb{Q}$

مثال ٦ : لتكن R حلقة إبدالية لها المميز p ، عدد أولى . برهن على أن راسم فوربينيس (Forbenius map) $x \to x^p$ هومومورفيزم حلقى من R إلى R .

البرهان : لجميع $x, y \in R$:

$$\varphi(xy) = (xy)^p \underset{R \text{ إبدالية}}{=} x^p y^p = \varphi(x)\varphi(y) \qquad (1)$$

$$\varphi(x+y) = (x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \ldots + \binom{p}{r}x^{p-r}y^r + \ldots + \binom{p}{p-1}xy^{p-1} + y^p$$

معامل الحد العام فى المفكوك السابق هو :

$$\binom{p}{r} = \frac{p!}{r!(p-r)!}$$

p يقسم $p!$ ، $p-r<p$ لجميع $1 \le r < p$ ، كما أن p عدد أولى فإذا قسم $r!(p-r)!$ فلابد أن يقسم أحد هذه العوامل وهذا مستحيل مما سبق . إذن p يقسم البسط ولا يقسم المقام فى $\frac{p!}{r!(p-r)!}$ وبهذا يصبح المفكوك

$$\varphi(x+y) = (x+y)^p = x^p + y^p = \varphi(x) + \varphi(y) \qquad (2)$$

من (1) ، (2) ينتج المطلوب مباشرة .

مثال ٧ : ليكن F حقلاً له المميز p ، عدد أولى. برهن على أن $K := \{x \in F \mid x^p = x\}$ حقل جزئى من F .

البرهان : $0^p = 0$ أى أن $0 \in K$ ، أى أن $K \neq \phi \quad (1)$

$1^p = 1$ أى أن $1 \in K$

ليكن $x, y \in K$ هذا يقتضى أن $x^p = x$ ، $y^p = y$. وبالتالى فإن :

$$(xy^{-1})^p \underset{F \text{ حقل}}{=} x^p y^{-p} = xy^{-1} \Rightarrow xy^{-1} \in K \qquad (2)$$

كذلك فإن :

$$(x-y)^p = x^p - \binom{p}{1}x^{p-1}y + \ldots + (-1)^r\binom{p}{r}x^{p-r}y^r + \ldots + (-1)^{p-1}xy^{p-1} + (-1)^p y^p$$

مثلما هى الحال فى المثال ٦ السابق مباشرة تختفى جميع الحدود ما عدا الحدين : الأول والأخير ويكون لدينا

$$(x-y)^p = x^p + (-1)^p y^p$$

لدينا حالتان : (أ) $p=2$

$$(x-y)^2 = x^2 + (-1)^2 y^2 = x^2 + y^2 = x^2 - y^2$$

(ب) $p \neq 2$ أى أن p عدد أولى فردى ، ويكون

$$(x-y)^p = x^p - y^p$$

فى الحالتين $(x-y)^p = x^p - y^p$

أى أن : (3) $x-y \in K$

من (1) ، (2) ، (3) ينتج المطلوب مباشرة .

<u>مثال ٨</u> : ليكن x ، y ينتميان إلى نطاق متكامل له المميز p ، عدد أولى .

برهن على أن :

(أ) $(x+y)^p = x^p + y^p$

(ب) $\forall n \in \mathbb{N} : (x+y)^{p^n} = x^{p^n} + y^{p^n}$

واوجد عنصرين x ، y فى حلقة مميزها 4 بحيث يكون $(x+y)^4 \neq x^4 + y^4$

<u>الحل</u> :

(أ) تماماً كما فى المثالين السابقين مباشرة

(ب) بالاستقراء الرياضى على n

$n=1$: صحيحة من (أ)

$n \to n+1$:

$$(x+y)^{p^{n+1}} = \left((x+y)^{p^n}\right)^p$$

$$= \left(x^{p^n}+y^{p^n}\right)^p = \left(x^{p^n}\right)^p + \binom{p}{1}\left(x^{p^n}\right)^{p-1} y^{p^n} + \ldots$$

فرض الاستقراء

$$+\binom{p}{r}\left(x^{p^n}\right)^{p-r}\left(y^{p^n}\right)^r + \ldots + \binom{p}{p-1} x^{p^n}\left(y^{p^n}\right)^{p-1} + \left(y^{p^n}\right)^p$$

وكما سبق فى المثالين السابقين مباشرة تختفى جميع الحدود من الفكوك السابق فيما عدا الحد الأول والحد الأخير ، ويكون لدينا :

$$(x+y)^{p^{n+1}} = \left(x^{p^n}\right)^p + \left(y^{p^n}\right)^p = x^{p^{n+1}} + y^{p^{n+1}}$$

والآن لنأخذ $x = y = 1$ فى الحلقة ذات المميز 4 فنحصل على :

$$(1+1)^4 = 2^4 = 0 \neq 2 = 1^4 + 1^4$$

١-٢ امتداد (اتساع) الحقول **Field extensions**

١-٢-١ تعريف : الزوج (K, k) المكون من حقل K ، وحقل جزئى k من K يسمى **امتداد (اتساع) حقل** (field extension) وسنكتب عادة $k \subset K$ بدلاً من (K, k) . ويقال أحياناً إن الحقل K امتداد للحقل k .

ليكن $k \subset K$ امتداد حقل ، وبهذا يكون K مع الراسمين :

$$\begin{array}{c} K \times K \to K \\ (x, y) \mapsto (x+y) \end{array} \quad , \quad \begin{array}{c} k \times K \to K \\ (a, k) \mapsto ak \end{array}$$

k - فراغاً خطياً (أى فراغاً خطياً على الحقل k)

يسمى $[K : k] := \dim_k(K)$ **درجة** (degree) (وتكتب deg) امتداد الحقل $k \subset K$.

($\dim_k(K)$ هو بعد الفراغ الخطى K على الحقل k)

يقال إن امتداد الحقل $k \subset K$ **منته** (finite) إذا كان $[K : k] < \infty$

ويقال لحقل L إنه حقل بينى (intermediate field) فى امتداد حقل $k \subset K$ عندما يكون L حقلاً جزئياً من K و k حقلاً جزئياً من L .

١-٢-٣ ملحوظة : ليكن $K \supset k$ اتساع حقل . عندئذ فإن :

$$[K : k] = 1 \Leftrightarrow K = k$$

البرهان : $[K:k]=1 \Leftrightarrow 1$عنصر الوحدة فى K يكون أساساً للفراغ الخطى K على k

$$\Leftrightarrow \quad K = 1.k = k$$

١-٢-٤ نظرية الدرجة Degree Theorem

إذا كان L حقلاً بينياً فى امتداد حقل $K \supset k$ فإن :

$$[K : k] = [K : L][L : k]$$

وعلى وجه الخصوص فإن امتداد الحقل $K \supset k$ يكون منتهياً إذا كان وفقط إذا كان كلا الامتدادين $K \supset L$ ، $L \supset k$ منتهياً . وإذا كان $\{x_1,...,x_m\}$ أساساً للفراغ الخطى L على k ، وكان $\{y_1,...,y_n\}$ أساساً للفراغ الخطى K على L فإن العناصر $x_i y_j$ حيث $i \in \{1,...,m\}$ ، $j \in \{1,...,n\}$ تبنى أساساً للفراغ الخطى K على k

البرهان :

(1) $[K : k] = \dim_k(K) \geq \dim_k(L) = [L : k] = \infty \Leftarrow [L : k] = \infty$

(2) $[K : k] = \dim_k(K) \geq \dim_L(K) = [K : L] = \infty \Leftarrow [K : L] = \infty$

(٣) ليكن $L \supset k$ ، $K \supset L$ اتساعى (امتدادى) حقلين منتهيين ، $\{x_1,...,x_m\}$ أساساً للفراغ الخطى L على k ، $\{y_1,...,y_n\}$ أساساً للفراغ الخطى K على L .

المطلوب البرهنة على أن العناصر $x_i y_j$ ، $i \in \{1,...,m\}$ ، $j \in \{1,...,n\}$ تبنى أساساً للفراغ الخطى K على k .

العناصر المذكورة تبنى نظاماً منشئاً (مولداً) (generating system) لأنه لكل $y \in K$ يوجد $b_1,...,b_n \in L$ بحيث يكون $y = \sum_{j=1}^{n} b_j y_j$ ولكل $j \in \{1,...,n\}$

يوجد $a_{1j},...,a_{mj} \in k$ بحيث يكون $b_j = \sum_{i=1}^{m} a_{ij} x_i$ ، وهكذا يكون

$$y = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_i y_j \ , \ a_{ij} \in k$$

وهذه العناصر أيضاً مستقلة خطياً (linearly independent) على k ، لأنه من

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_i y_j = 0 \ , \ a_{ij} \in k$$ ينتج أن $\sum_{i=1}^{m} a_{ij} x_i = 0$ لكل $j \in \{1,...,n\}$

(لأن $\{y_1,...,y_n\}$ أساس للفراغ الخطى K على L) ، ومن ثم فإن $a_{ij} = 0$ لكل $i \in \{1,...,m\}$ ، ولكل $j \in \{1,...,n\}$ (لأن $\{x_1,...,x_m\}$ أساس للفراغ الخطى L على k) نهاية البرهان .

والآن : ليكن $E \supset F$ امتداد حقل . بعبارة مكافئة نقول E امتداد حقل لـــ F . يقال إن E له درجة n على F ونكتب $[E : F] = n$ إذا كان E له البعد n كفراغ خطى على F .

<u>١-٢-٥ نتيجة</u> :

ليكن $K \supset L$ اتساع حقل منتهياً .

(١) لكل حقل بينى L فى امتداد حقل $K \supset k$ بحيث يكون $[K : L] = [K : k]$ فإن $L = k$

<u>البرهان</u> :

$$[K : k] = [K : L][L : k] = [K : L] \Rightarrow [L : k] = 1$$

ومن (١-٢-٣) يكون $L = k$

(٢) إذا كان $[K : k]$ عدداً أولياً فإن امتداد الحقل $K \supset k$ لايوجد فيه أى حقل بينى فعلى . وعلى سبيل المثال فلا يوجد أى حقل بينى "فعلى" فى اتساع الحقل $\mathbb{C} \supset \mathbb{R}$ لأن درجة هذا الاتساع "2" (1 ، i يكونان أساساً للفراغ الخطى $\mathbb{C}$ على $\mathbb{R}$)

٣-١ الضم (الإلحاق) للحلقة وللحقل Ring adjunction and field adjunction

١-٣-١ تعريف :

ليكن $k \subset K$ اتساع حقل ، A مجموعة جزئية من K . يسمى :

$$k[A] := \cap\{R : \quad R,k \cup A \subset R \text{ حلقة جزئية من } K\}$$

$$k(A) := \cap\{L : \quad L,k \cup A \subset L \text{ حقل جزئى من } K\}$$

الحلقة الجزئية والحقل الجزئى على الترتيب من K المنشأين من A على k .

فى حالة $A = \{a_1,...,a_n\}$ نكتب غالباً $k[a_1,...,a_n]$ بدلاً من $k[A]$ ، $k(a_1,...,a_n)$ بدلاً من $k(A)$.

١-٣-٢ ملحوظة :

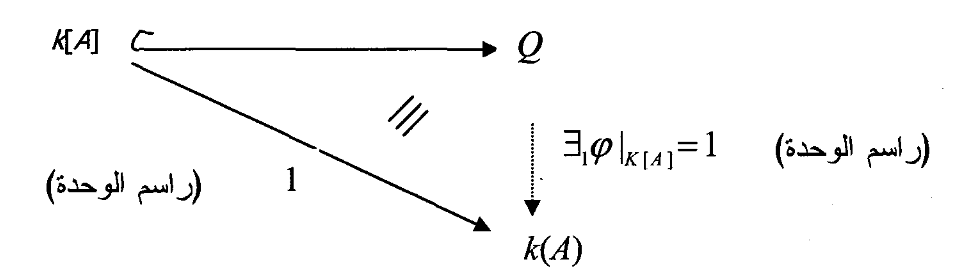
ليكن $k \subset K$ امتداد حقل . عندئذ فإن :

(١) لكل مجموعة جزئية A من K يكون $k(A)$ حقل القسمة لـــ $k[A]$

(٢) لكل $a \in K$ يكون $k[a] = \{f(a) \mid f \in k[X]\}$

(٣) لكل مجموعتين جزئيتين A ، B من K : $k(A \cup B) = (k(A))(B)$

البرهان : (١)



نعتبر الحلقة $k[A]$ كحلقة جزئية من حقل قسمتها Q . وهكذا يوجد بسبب الخاصة الكونية (العالمية) – مونومورفيزم واحد بالضبط $\varphi : Q \to k(A)$ بحيث يكون $\varphi|_{k[A]} = 1$. φ راسم غامر (شامل ، فوقى) كذلك ، لأن $\varphi(Q)$ حقل جزئى من $k(A)$ (أيضاً من K) ويتحقق :

$k \cup A = \varphi(k \cup A) \subset \varphi(Q)$ ومن حيث إن $k(A)$ تقاطع جميع الحقول الجزئية من K التى تحتوى على $k \cup A$ ، أى هو أصغر هذه الحقول الجزئية فينتج أن $k(A) \subset \varphi(Q)$. وبالتالى فإن $\varphi(Q) = k(A)$ أى أن φ شامل (غامر) . وبهذا يكون الحقل $k(A)$ متشاكلاً مع حقل القسمة Q ويكون هو نفسه حقل القسمة لـــ $k[A]$.

(٢) المجموعة $R := \{f(a) \mid f \in k[X]\}$

حلقة جزئية من K لأن $a \in R$ (لأن $f = X \in k[X]$) أى أن $R \neq \phi$.

$$f(a)g(a) = (f.g)(a) \in R \Leftarrow f-g, f.g \in k[X] \Leftarrow f, g \in k[X] \Leftarrow f(a), g(a) \in R$$
حلقة $k[X]$

وكذلك $f(a) - g(a) = (f-g)(a) \in R$

كذلك فإن $k \cup \{a\} \subset R$. ومن حيث إن $k[a]$ أصغر حلقة جزئية من K تحتوى على $k \cup \{a\}$ فيكون $k[a] \subset R$ (1) .

ولكن لكل حلقة جزئية S من K بحيث إن $k \cup \{a\} \subset S$ فإنه من الواضح أن $R \subset S$ فيكون $R \subset k[a]$ (2) . من (1) ، (2) ينتج أن $R = k[a]$.

(٣) $k(A \cup B) = \cap\{L \mid k \cup (A \cup B) \subset L$, L حقل جزئى من $K\}$

$= \cap\{L \mid k(A) \cup B \subset L$, L حقل جزئى من $K\}$

$= (k(A))(B)$

<u>١-٣-٣ تعريف</u> :

يقال لاتساع (امتداد) الحقل $k \subset K$ **<u>بسيط</u>** (simple) إذا وجد $a \in K$ بحيث يكون $K = k(a)$. ويسمى a فى هذه الحالة **<u>عنصراً بدائياً</u>** (primitive element) لاتساع الحقل $k \subset K$.

<u>١-٣-٤ مثال</u> :

واضح أن $\mathbb{C} \supset \mathbb{R}[i]$. كذلك فإن أية حلقة جزئية من $\mathbb{C}$ تحتوى على $\mathbb{R}$ ، i تحتوى $\mathbb{C}$. وبهذا يكون تقاطع هذه الحلقات الجزئية يحتوى على $\mathbb{C}$. ومن ثم فإن

$\mathbb{R}[i]=\mathbb{C}$. وبهذا يكون $\mathbb{R}[i]$ حقلاً ويكون $\mathbb{R}(i)=\mathbb{R}[i]=\mathbb{C}$. ومن ثم يكون العدد المركب i عنصراً بدائياً لاتساع الحقل $\mathbb{C}\supset\mathbb{R}$.

١-٤ العناصر الجبرية والمتسامية

Algebraic and Transcendental Elements

١-٤-١ تعريف :

ليكن $K\supset k$ امتداد حقل .

يقال لعنصر $a\in K$ إنه **جبرى** (algebraic) **على k** ، إذا وجدت كثيرة حدود $f\in k[X]\setminus\{0\}$ بحيث يكون $f(a)=0$. فإذا كانت f الوحيدة المطبعة غير القابلة للتبسيط (للتحليل) ذات الدرجة (الصغرى) n قيل إن a جبرى على k من درجة n .

وإذا لم توجد مثل هذه كثيرة الحدود فيقال إن العنصر **متسام**(transcendental)**على k** .

وتسمى عناصر $\mathbb{C}$ الجبرية على $\mathbb{Q}$ **الأعداد الجبرية** (algebraic numbers) .

وسنرى أن هذه الأعداد تكون حقلاً بينياً فى $\mathbb{Q}\subset\mathbb{C}$

١-٤-٢ ملحوظة :

ليكن $K\supset k$ امتداد حقل ، $a\in K$ ،

$$\varphi_a : k[X]\to K$$
$$f\mapsto f(a)$$

واضح تماماً أن φ_a هومومورفيزم حلق .

a جبرى على k $\Leftrightarrow \exists f\neq 0, f\in k[X]: f(a)=0 \Leftrightarrow$ ليس واحداً لواحد φ_a

a متسام على k $\Leftrightarrow \nexists f\neq 0, f\in k[X]: f(a)=0 \Leftrightarrow$ واحد لواحد φ_a

١-٤-٣ ملحوظة :

ليكن $K\supset k$ امتداد حقل ، وليكن $a\in K$ متسامياً على k . عندئذ فإن :

(١) الحلقة $k[a]$ تتشاكل مع حلقة كثيرات الحدود $k[X]$

(٢) الحقل $k(a)$ يتشاكل مع $k(X)$ حقل الدوال الكسرية (النسبية)

(٣) $[k(a):k]=\infty$

البرهان :

(١) الراسم $\begin{array}{l} k[X] \to k[a] \\ f \mapsto f(a) \end{array}$ هومومورفيزم غامر (شامل ، فوقى) ولأن a متسام على k يكون كذلك واحداً لواحد . أى هو أيزومورفيزم .

(٢) من (١) $k[a]$ تتشاكل مع $k[X]$ ، ومن (١-٣-٢) $k(a)$ هو حقل القسمة لـــ $k[a]$ ، ومن تعريف $k(X)$ ينتج المطلوب مباشرة

(٣) من(١)$k[a]$ يتشاكل مع$k[X]$، ولأنه لجميع $n \in \mathbb{N}$ تكون كثيرات الحدود X،X^2،...، X^n مستقلة خطياً فيكون $\dim_k(k[X]) = \infty$ أى أن$\infty=\dim_k(k(X))=\dim_k(k(a))=[k(a):k]$

١-٤-٤ نظرية :

ليكن $K \supset k$ امتداد حقل ، وليكن $a \in K$ عنصراً متسامياً على k .

عندئذ فإن :

(١) a^2 عنصر متسام على k

(٢) $k(a^2) \subsetneq k(a)$

(٣) امتداد الحقل $k(a) \supset k$ يحتوى عدداً غير منته من الحقول البينية .

البرهان :

(١) إذا كان a^2 جبرياً على k فإنه توجد كثيرة حدود $f \in k[X] \setminus \{0\}$ بحيث يكون $f(a^2) = 0$. وعندئذ فإن a تكون صفراً لكثيرة الحدود $0 \neq g := f(X^2)$ أى أن a جبرى على k : تناقض .

(٢) من (١-٣-٢) إذا كان $a \in k(a^2)$ فإنه ينتج أنه يوجد $f, g \in k[X]$ بحيث يكون : $a = \dfrac{f(a^2)}{g(a^2)}$. وبالتالى يكون a صفراً لكثيرة الحدود: $h := Xg(X^2) - f(X^2)$.

و h لايمكن أن تساوى الصفر لأن $\deg(f(X^2)) \neq \deg(Xg(X^2))$ وبهذا يكون a جبرياً على k . وهذا تناقض .

(٣) من (١) واضح أنه بالاستقراء الرياضى يكون $a^n, n = 3, 4, \ldots$ عنصراً متسامياً على k ومن (٢) ينتج أن $k \subset \ldots \subsetneq k(a^3) \subsetneq k(a^2) \subsetneq k(a)$

١-٥ كثيرة الحدود الصغرى The minimal polynomial

١-٥-١ ملحوظة :

ليكن $K \supset k$ امتداد حقل ، $a \in K$ ، $\varphi_a : k[X] \to K$ هومومورفيزما بحيث إن $\varphi_a(f) = f(a)$ لجميع $f \in k[X]$. إذا كان a جبريا على k فإنه يوجد بالضبط كثيرة حدود مطبعة وحيدة $f_a \in k[X]$ بحيث يكون $Ker(\varphi_a) = [f_a]$

البرهان : φ_a هومومورفيزم لأن :

$$\forall f, g \in k[X] : \varphi_a(f+g) = (f+g)(a) = f(a) + g(a) = \varphi_a(f) + \varphi_a(g)$$

$$\varphi_a(f.g) = (f.g)(a) = f(a).g(a) = \varphi_a(f).\varphi_a(g)$$

والآن لأن a جبرى على k فينتج من (١-٤-٢) أن $Ker(\varphi_a) \neq \{0\}$، ينتج من (٢-١-١١) فى نظرية الحلقات المطلوب مباشرة (تذكر أن نواة الهومورفيزم الحلقى تكون مثاليا) .

١-٥-٢ تعريف :

ليكن $K \supset k$ امتداد حقل ، $a \in K$ جبريا على k . ينتج من (١-٥-١) أنه توجد كثيرة حدود مطبعة وحيدة $f_a \in k[X]$ حيث $[f_a] = \{f \in k[X] | f(a) = 0\}$ تسمى <u>كثيرة الحدود الصغرى</u> من a على k. (The minimal polynomial for a over k) .

١-٥-٣ نظرية :

ليكن $K \supset k$ امتداد حقل ، $a \in K$ جبريا على k ،

$$A := \{f \in k[X] : f(a) = 0\}$$

عندئذ فإنه لكل كثيرة حدود مطبعة $g \in A$ تكون التقريرات الآتية متكافئة :

(١) g هى كثيرة الحدود الصغرى من a على k

(٢) لجميع $f \in A \setminus \{0\}$: $\deg(g) \le \deg(f)$

(٣) g غير قابلة للتبسيط فى $k[X]$

وهكذا فإن كثيرة الحدود $g \in k[X]$ تكون كثيرة الحدود الصغرى من a على k إذا كانت وفقط إذا كانت g مطبعة ، غير قابلة للتبسيط فى $k[X]$ ، $g(a) = 0$

<u>البرهان</u> : "(١) $\Leftarrow$ (٢)" : إذا كانت g هى كثيرة الحدود الصغرى من a على k فإن $[g] = A$ ومن ثم فإن $\deg(g) \le \deg(f)$ لجميع $f \in A \setminus \{0\}$

"(٢) $\Leftarrow$ (٣)" : ليكن $g = fh$ حيث $f, h \in k[X]$. ينتج أن : $0 = g(a) = f(a)h(a)$ ولأن k حقل فإن $f \in A$ أو $h \in A$. ومن (٢) $\deg(g) \le \deg(f)$ ومن ثم فإن $h \in k^*(= k \setminus \{0\})$ أو $\deg(g) \le \deg(h)$ ، ومن ثم فإن $f \in k^*$.

"(٣) $\Leftarrow$ (١)" : لتكن f_a هى كثيرة الحدود الصغرى من a على k . عندئذ فإن $g \in [f_a]$ ، بحيث إنه يوجد $h \in k[X]$ ، $g = hf_a$. ولأن g غير قابلة للتبسيط (= غير قابلة للتحليل) فى $k[X]$ ينتج أن $h \in k^*$. ولأن كلا من g ، f_a مطبعة فإن $h = 1$ ويكون $g = f_a$

<u>١-٥-٤ مثال</u> :

برهن على أنه لكل عدد أولى p تكون كثيرة الحدود $X^2 - p$ هى كثيرة الحدود الصغرى من $\sqrt{p}$ على $\mathbb{Q}$.

<u>البرهان</u> : نعلم من (٣-٦-٣) فى نظرية الحلقات أن كثيرة الحدود $X^n - p$ حيث p عدد أولى غير قابلة للتبسيط (للتحليل) فى $\mathbb{Q}[X]$.

كذلك فإن $(\sqrt{p})^2 - p = 0$ ، أى أن $\sqrt{p}$ صفر لكثيرة الحدود $X^2 - p$ و $X^2 - p$ مطبعة ، فمن (١-٥-٣) ينتج المطلوب مباشرة .

<u>١-٥-٥ نظرية</u> :

ليكن $k \subset K$ امتداد حقل ، $a \in K$ جبرياً على k . f هى كثيرة الحدود الصغرى من a على k . عندئذ فإن :

$$k[a]=k(a)\cong k[X]/[f] \quad (١)$$

$$[k(a):k]=\deg(f) \quad (٢)$$

(٣) إذا كان $m:=\deg(f)$ فإن $\{1,a,...,a^{m-1}\}$ تكون أساساً للفراغ الخطى $k(a)$ على k .

<u>البرهان</u> : اعتبر

$$\varphi: k[X]\to k[a]$$
$$g\mapsto g(a)$$

واضح أن φ هومومورفيزم ، غامر (شامل ، فوقى) ،

$$Ker(\varphi)=\{g\in k[X]:\varphi(g)=0\}$$
$$=\{g\in k[X]:g(a)=0\}$$

تذكر أن k حقل يقتضى أن $k[X]$ نطاق مثاليات أساسية ، $Ker(\varphi)$ مثالى فى $k[X]$ ، أى أن $Ker(\varphi)$ مثالى أساسى فى $k[X]$ ، وهو يساوى المثالى المتولد من كثيرة الحدود الصغرى من a على k ، أى أن $Ker(\varphi)=[f]$. وبتطبيق نظرية الهومومورفيزم ينتج أن : $k[a]\cong k[X]/[f]$. ولأن f كثيرة حدود صغرى ، فهى غير قابلة للتبسيط وينتج من (٣-٢-٩) فى نظرية الحلقات أن المثالى $[f]$ مثالى أعظم ، ولأن $k[X]$ حلقة إبدالية لها عنصر الوحدة فينتج من (١-٣-١١) أن $k[a]$ حقل أى أن $k[a]=k(a)\cong k[X]/(f)$.

(٢) ، (٣) : من (١) لدينا : $k[a]=\{g(a):g\in k[X],\deg(g)<\deg(f)\}$ (انظر مثال ١٩ فى (٢-٢-٨) من نظرية الحلقات). ولأن φ راسم غامر (شامل ، فوقى) فإنه لكل $b\in k[a]$ يوجد $g\in k[X]$ بحيث يكون $b=g(a)$. وباختيار $q,r\in k[X]$ بحيث يكون $g=qf+r,\deg(r)<\deg(f)$ نحصل على $b=g(a)=r(a)$. والآن لكل $b\in k[a]$ يوجد $\beta_0,\beta_1,...,\beta_{m-1}\in k$ بحيث يكون $b=\beta_0 1+\beta_0 a+...+\beta_{m-1}a^{m-1}$

(لأن $\deg(r) < \deg(f) = m$) ، أى أن العناصر 1 ، a ، ... ، a^{m-1} تنشئ الفراغ الخطى $k[a]$ على k . وإذا كانت العناصر 1 ، a ، ... ، a^{m-1} مرتبطة خطياً (= معتمدة خطياً = غير مستقلة خطياً) فيكون لدينا كثيرة حدود $g \in k[X] \setminus \{0\}$ ، $\deg(g) < \deg(f)$ ، a صفر لكثيرة الحدود هذه . وهذا تناقض لأن f كثيرة الحدود الصغرى من a على k (انظر (١-٥-٣))

١-٦ الامتدادات الجبرية للحقول Algebraic field extensions

١-٦-١ تعريف :

يسمى امتداد الحقل $K \supset k$ **امتداد حقل جبرياً** (algebraic field extension) إذا كان كل عنصر فى K جبرياً على k . **ويسمى امتداد حقل متسامياً** (transcendental field extension) إذا لم يكن جبرياً ، أى عندما يكون هناك عنصر $a \in K$ متسامياً على k .

١-٦-٢ نظرية :

ليكن $K \supset k$ امتداد حقل . عندئذ فإن :

(١) إذا كان امتداد الحقل $K \supset k$ منتهياً ، فإنه يكون جبرياً ، ويوجد a_1 ، ... ، a_n عناصر فى K بحيث يكون $K = k(a_1,...,a_n)$

(٢) إذا وجدت عناصر $a_1,...,a_n \in K$ جبرية على k بحيث يكون $K = k(a_1,...,a_n)$ فإن امتداد الحقل يكون منتهياً وبالتالى جبرياً .

البرهان : (١) إذا كان m هو بعد الفراغ الخطى K على k ، فإنه لأى عنصر $a \in K$ تكون العناصر 1، a ، a^2 ، ... ، a^m مرتبطة (= معتمدة = غير مستقلة) خطياً على k . ومن ثم فإنه لكل $a \in K$ توجد كثيرة حدود $f \in k[X] \setminus \{0\}$ بحيث يكون $f(a) = 0$. وعلاوة على ذلك فإن $K = k(a_1,...,a_n)$ لكل أساس $(a_1,...,a_n)$ للفراغ الخطى K على k

(٢) البرهان بالاستقراء الرياضى : إذا كان $a \in K$ جبرياً على k وكان $K = k(a)$ ، فإنه ينتج من (١-٥-٥) أن $[K : k] < \infty$.

ليكن $n \in \mathbb{N} \setminus \{0\}$ ، وليكن الادعاء صحيحاً لجميع الحقول البينية $L \supset k$ ، $L = k(a_1,...,a_n)$

حيث a_1 ، ... ، a_n جبرية على k . عندئذ فإنه إذا كان $K = k(a_1,...,a_{n+1})$ حيث

$a_1,...,a_{n+1} \in K$ جبرية على k . فينتج أن :

$$[K : k] = [k(a_1,...,a_n)(a_{n+1}) : k(a_1,...,a_n)][k(a_1,...,a_n) : k] < \infty$$

(لأن a_{n+1} جبرى على $k(a_1,...,a_n)$ ومن (١-٢-٤) و (١-٥-٥)) أى أن امتداد الحقل المعنى منته ، وبالتالى من (١) فهو جبرى .

<u>١-٦-٣ استنتاج</u> :

ليكن L حقلاً بينياً فى امتداد حقل $K \supset k$. عندئذ فإن امتداد الحقل $K \supset k$ يكون جبرياً إذا كان وفقط إذا كان الامتدادان : $K \supset L$ ، $L \supset k$ جبريين .

<u>البرهان</u> : من الواضح أنه إذا كان $K \supset k$ جبرياً فإن $L \supset k$ ، $K \supset L$ جبريين .

والآن ليكن الامتدادان $L \supset k$ ، $K \supset L$ جبريين ، وليكن $a \in K$. عندئذ فإنه يوجد $b_0,...,b_n \in L$ بحيث إن $a^{n+1} + b_n a^n + ... + b_1 a + b_0 = 0$ ، ويكون a جبرياً على $k(b_0,...,b_n)$.

ولأن $L \supset k$ جبرى فتكون b_0 ، ... ، b_n جبرية على k ونحصل من (١-٦-٢) على

$$[k(a):k] \le [k(b_0,...,b_n)(a):k] = [k(b_0,...,b_n)(a):k(b_0,...,b_n)][k(b_0,...,b_n):k] < \infty$$

١-٢-٤

أى أن $[k(a):k]$ منته ، ومن ثم فهو جبرى ، وبالتالى يكون $a \in K$ جبرياً على k ، ويكون $K \supset k$ جبرياً .

<u>١-٦-٤ استنتاج</u> :

ليكن $K \supset k$ امتداد حقل ، L مجموعة كل العناصر فى K الجبرية على k . عندئذ فإن :

(١) L حقل بينى فى الامتداد $K \supset k$

(٢) الامتداد $L \supset k$ جبرى

(٣) إذا كان $a \in K$ جبرياً على L ، فإن $a \in L$

البرهان : (١) واضح أن $k \subset L$. ليكن $a,b \in L$. من (١-٦-٢) ينتج أن : امتداد الحقل $k(a,b) \supset k$ جبرى. لأن $a-b$ وكذلك ab^{-1} (إذا كان $b \neq 0$) عنصران فى $k(a,b)$ فإن $a-b$ ، ab^{-1} (إذا كان $b \neq 0$) يقعان فى L إذا كان $a,b \in L$

(٢) واضح من تعريف L

(٣) إذا كان $a \in K$ جبرياً على L فمن (١-٦-٢) يكون الامتداد $L(a) \supset L$ جبرياً . ومن (٢) السابقة مباشرة ومن (١-٦-٣) يكون $L(a) \supset k$ جبرياً ، أى أن a جبرى على k ، وبالتالى $a \in L$.

١-٦-٥ ملحوظة :

المجموعة $\overline{\mathbb{Q}}$ (مجموعة كل الأعداد الجبرية) هى حقل بينى فى الامتداد $\mathbb{C} \supset \mathbb{Q}$ ، والامتداد $\overline{\mathbb{Q}} \supset \mathbb{Q}$ جبرى ، ولايوجد عدد فى $\mathbb{C}$ يكون جبرياً على $\overline{\mathbb{Q}}$ ولايقع فى $\overline{\mathbb{Q}}$.

١-٧ إنشاء امتدادات الحقول Construction of field extensions

١-٧-١ نظرية :

إذا كان k حقلاً ، f كثيرة حدود ليست ثابتاً معرفة على $k[X]$ ، فإنه يوجد K حقل فوقى لـــ k ، $a \in K$ بحيث يكون $f(a) = 0$

البرهان : إذا كان p عاملاً لـــ f غير قابل للتبسيط ، فإن المثالى $[p]$ فى $k[X]$ يكون مثالياً أعظم (انظر (٣-٢-٩)) ، ومن (١-٣-١١) يكون $K := k[X]/[p]$ حقلاً .

نعتبر الآن الإبيمورفيزم الطبيعى

$$\rho : k[X] \to k[X]/[p]$$

وتحديد ρ على k يكون مونومورفيزم ، لأنه لعنصر $x \in k^*$

$$x + [p] = \rho(x) = [p] \Rightarrow x \in [p]$$

وبالتالى فإن : $1=x^{-1}x\in[p]$ ، ومن ثم فإن $[p]=k[X]$ وهذا يناقض أن $[p]$ مثالى أعظم فى $k[X]$ وبالتالى يكون p ليس غير قابل للتبسيط أى قابلاً للتبسيط وهذا تناقض .

إذن نواة ρ محدداً على k هى $\{0\}$ ويكون ρ راسماً أحادياً (وبالتالى مونومورفيزماً).

ومن ثم فيمكننا أن نوحد (identify) $\rho(x)$ مع كل $x\in k$ ويمكن أن نعتبر k حقلاً جزئياً من K . العنصر $a:=\rho(X)\in K$ يكون صفراً لــ p ومن ثم لــ f لأنه :

$$p(a)=p(\rho(X))=\rho(p)=p+[p]=[p]=\bar{0}$$

($[p]$ هو صفر $k[X]/[p]$)

١-٨ حقول التشقيق وتمديد أيزومورفيزمات (تشاكلات) الحقول

Splitting fields and extension of field-isomorphisms

نريد أن نبرهن هنا على أنه لكل كثيرة حدود ليست ثابتة $f\in k[X]$ ، حيث k حقل ، يوجد حقل فوقى أصغر وحيد – بدون حساب الأيزومورفيزمات – فيه تتحلل f إلى عومل خطية (أى عوامل من الدرجة الأولى

١-٨-١ تعريف :

يقال إن امتداد الحقل $K\supset k$ حقل تشقيق (splitting field) لكثيرة حدود ليست ثابتة $f\in k[X]$ (يقال أيضاً إن K حقل تشقيق f على k) إذا تحقق

(١) f تتشقق على K فى عوامل خطية ، أى أنه يوجد $a_1,\ldots,a_n,b\in K$ بحيث يكون :

$$f=b(X-a_1)\ldots(X-a_n)$$

(٢) K هو الأصغر بالنسبة إلى (١) أى أن f لاتشقق فى حقل بينى فعلى فى امتداد الحقل $K\supset k$ فى عوامل خطية .

١-٨-٢ مثال :

$\mathbb{C}\supset\mathbb{R}$ هو حقل تشقيق لكثيرة الحدود $X^2+1\in\mathbb{R}[X]$. بينما $\mathbb{Q}(i)\supset\mathbb{Q}$ هو حقل تشقيق لكثيرة الحدود $X^2+1\in\mathbb{Q}[X]$

١-٨-٣ نظرية :

ليكن k ،k' حقلين ، وليكن $\varphi: k \to k'$ تشاكلا (أيزومورفيزما) ، $\Phi: k[X] \to k'[X]$ التشاكل المناظر لحلقات كثيرات الحدود .

ولتكن $f \in k[X]$ غير قابلة للتبسيط (للتحليل) ، وليكن a صفراً لـ f فى حقل فوقى لـ k ، a' صفراً لـ $f' := \Phi(f)$ فى حقل فوقى لـ k' . عندئذ يوجد بالضبط أيزومورفيزم وحيد

$$\widehat{\varphi}: k(a) \to k'(a'), \quad \widehat{\varphi} \,|\, k = \varphi, \; \widehat{\varphi}(a) = a'$$

البرهان :

إذا حقق $\widehat{\varphi}$ الخصائص السابقة ، فسيحقق :

$$\forall g \in k[X]: \quad \widehat{\varphi}(g(a)) = \Phi(g)(a') \qquad (*)$$

لأنه إذا كان $g = \lambda_0 + \lambda_1 X + \ldots + \lambda_n X^n, \lambda_1, \ldots, \lambda_n \in k$ فإن

$$\begin{aligned}
\widehat{\varphi}(g(a)) &= \widehat{\varphi}(\lambda_0 + \lambda_1 a + \ldots + \lambda_n a^n) \\
&= \widehat{\varphi}(\lambda_0) + \widehat{\varphi}(\lambda_1)\widehat{\varphi}(a) + \ldots + \widehat{\varphi}(\lambda_n)\widehat{\varphi}(a^n) \\
&= \varphi(\lambda_0) + \varphi(\lambda_1)a' + \ldots + \varphi(\lambda_n)(a')^n \\
&= \Phi(g)(a')
\end{aligned}$$

أى أن الشكل الآتى يكون إبداليا (commutative)

$$\begin{array}{ccccc}
g \in & k[X] & \xrightarrow{\quad \Phi \quad} & k'[X] & \ni h \\
\big\downarrow & \big\downarrow \rho & /\!/\!/ & \big\downarrow \rho' & \big\downarrow \\
g(a) & \in k(a) & \xrightarrow{\quad \widehat{\varphi} \quad} & k'(a') & \ni h(a')
\end{array}$$

وإذا وجد أيزومورفيزم آخر ψ يجعل الشكل إبداليا يكون لدينا :

$$\widehat{\varphi} o \rho = \psi o \rho \quad \Rightarrow \quad \widehat{\varphi} = \psi$$

ρ غامر (شامل)

أى أن $\widehat{\varphi}$ وحيد (إن وجد)

والآن نثبت أنه يوجد بالفعل هذا الـ $\widehat{\varphi}$:

واضح أن $f \in Ker(\rho)$ (لأن $Ker(\rho)=\{f \in k[X]: f(a)=0\}$)

أى أن $[f] \subset Ker(\rho)$ ولكن f غير قابلة للتبسيط فيكون $[f]$ مثالياً أعظم وبالتالى يكون $[f]=Ker(\rho)$.

والآن

$$\rho'(\Phi(f))=(\Phi(f))(a')=0 \Rightarrow \Phi(f) \in Ker(\rho')$$

وينتج من مثال ٣٥ فى (١-٢-٨) فى نظرية الحلقات أنه يوجد هومومورفيزم غامر (شامل ، فوقى) $\widehat{\varphi}: k(a) \to k'(a')$ يجعل الشكل السابق إبدالياً . ولأن $\widehat{\varphi}$ هومومورفيزم غامر من حقل على حقل فلابد أن يكون $\widehat{\varphi}$ أيزومورفيزماً .

(تذكر أنه إذا كان هناك هومومورفيزم بين حقلين فنواة الهومومورفيزم إما أن تكون الحقل النطاق أو $\{0\}$ حيث $\{0\}$ هو صفر حقل النطاق) .

والآن إذا كان $b \in k$ فإن $b=\rho(b)$ ، ونحصل على :

$$\widehat{\varphi}(b)=\widehat{\varphi}(\rho(b))=(\widehat{\varphi} o \rho)(b)=(\rho' o \Phi)(b)=\rho'(\Phi(b))=\rho'(\varphi(b))=\varphi(b),$$

$$\widehat{\varphi}(a)=\widehat{\varphi}(\rho(X))=(\widehat{\varphi} o \rho)(X)=(\rho' o \Phi)(X)=\rho'(\Phi(X))=\rho'(X)=a'$$

أى أن $\widehat{\varphi}$ تحقق الخصائص المطلوبة

١-٨-٤ استنتاج :

ليكن $K \supset k$ امتداد حقل ، $a, a' \in K$ جبريين على k . إذا تطابقت كثيرتا الحدود الصغريان من a ، a' على k ، فإنه يوجد بالضبط أيزومورفيزم وحيد $\varphi: k(a) \to k(a')$ بحيث يكون $\varphi | k = 1_k$ ، $\varphi(a)=a'$ (1_k هو راسم الوحدة على k)

١-٨-٥ مثال :

كثيرة الحدود المطبعة $X^2-2\in\mathbb{Q}[X]$ غير قابلة للتبسيط (للتحليل) فى $\mathbb{Q}[X]$ و $\pm\sqrt{2}$ صفران لها ، فهى كثيرة الحدود الصغرى من $\pm\sqrt{2}$ على $\mathbb{Q}$. ومن (١-٨-٤) يوجد بالضبط أوتومورفيزم وحيد $\varphi:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{2})$ بحيث يكون $\varphi(\sqrt{2})=-\sqrt{2}$ ، $\varphi|\mathbb{Q}=1_{\mathbb{Q}}$. بالطبع فإن هناك أوتومورفيزم الوحدة على $\mathbb{Q}(\sqrt{2})$ الذى يرسم $\sqrt{2}$ فى $\sqrt{2}$.

ولأن كل أوتومورفيزم ψ على $\mathbb{Q}(\sqrt{2})$ له الخاصة :

$$2=1+1=\psi(1)+\psi(1)=\psi(1+1)=\psi(2)=\psi(\sqrt{2^2})=\psi(\sqrt{2})^2$$

ينتج أن $\psi(\sqrt{2})=\sqrt{2}$ أو $\psi(\sqrt{2})=-\sqrt{2}$

وبالتالى فإنه لايوجد أوتومورفيزمات أخرى على $\mathbb{Q}(\sqrt{2})$ ، يوجد فقط اثنان أوتومورفيزم الوحدة ، φ السابق .

<u>١-٨-٦ نظرية</u> :

ليكن k ، k' حقلين ، $\varphi:k\to k'$ تشاكلاً (أيزومورفيزماً) ، $\Phi:k[X]\to k'[X]$ الأيزومورفيزم المناظر لحقات كثيرات الحدود. ولتكن $f\in k[X]$ كثيرة حدود غير ثابتة. إذا كان $K\supset k$ حقل تشقيق لـــ f ، $K'\supset k'$ حقل تشقيق لـــ $f':=\Phi(f)$ ، فإنه يوجد أيزومورفيزم $\psi:k\to k'$ له الخصائص الآتية :

(١) $\psi|k=\varphi$

(٢) ψ يرسم مجموعة أصفار f فى K على مجموعة أصفار f' فى K' .

وعلى النقيض من التمديد فى (١-٨-٣) فإن ψ ليست وحيدة . وهذه هى نقطة البداية لنظرية جالوا .

<u>البرهان</u> : بالاستقراء الرياضى على r عدد أصفار f الموجودة فى $K\setminus k$

إذا كان $r=0$ فإن $K=k$ ، وبالتالى فإنه يوجد $a_1,\dots,a_n,c\in k$ بحيث يكون : $f=c(X-a_1)\dots(X-a_n)$ وينتج أن : $f'=\Phi(f)=\varphi(c)(X-\varphi(a_1))\dots(X-\varphi(a_n))$

وبهذا يحقق الأيزومورفيزم $\varphi : k \to k'$ الخصائص المطلوبة .

ليكن الآن $r \geq 1$ وليكن الادعاء صحيحاً لجميع k ، k' ، φ ، f ، K ، K' التى تحقق فروض النظرية ، وبالإضافة إلى هذا تقع $r-1$ على الأكثر من أصفار f فى $K \setminus k$.

والآن إذا حققت k ، k' ، φ ، f ، K ، K' فروض النظرية وكانت r من الأصفار لـ f : a_1 ، ... ، a_r تقع فى $K \setminus k$. فنعتبر كثيرة الحدود الصغرى p من a_1 على k .

هذه قاسم لـ f وبحيث يكون $p' := \Phi(p)$ قاسماً لـ $f' := \Phi(f)$. ولأن f' تتشقق فى عوامل خطية فى K' ، يكون لـ p' صفر هو a_1' فى K'. ومن (١-٨-٣) يوجد أيزومورفيزم $\bar{\varphi} : k(a_1) \to k'(a_1')$ بحيث يكون $\bar{\varphi} | k = \varphi$ ، $\bar{\varphi}(a_1) = a_1'$.

والآن بتطبيق فرض الاستقراء الرياضى على $k(a_1)$ ، $k'(a_1')$ ، $\bar{\varphi}$ ، f ، K ، K' ينتج المطلوب مباشرة .

<u>**١-٨-٧ نظرية**</u> :

ليكن k ، k' حقلين ، $\varphi : k \to k'$ تشاكلاً (أيزومورفيزما)، وليكن $\Phi : k[X] \to k'[X]$ التشاكل (الأيزومورفيزم) المناظر لحلقات كثيرات الحدود . ولتكن f كثيرة حدود ليست ثابتة فى $k[X]$.

إذا كان $K \supset k$ هو حقل تشقيق لـ f ، $K' \supset k'$ حقل تشقيق لـ $f' := \Phi(f)$ ، فإنه لكل صفر a يوجد عامل غير قابل للتبسيط لـ f فى K ، ليكن هو g ، ولكل صفر a' لـ $g' := \Phi(g)$ يوجد تشاكل (أيزومورفيزم) $\psi : K \to K'$ له الخصائص الآتية :

(١) ψ ترسم مجموعة أصفار f فى K على مجموعة أصفار f' فى K' .

(٢) $\psi(a) = a'$

(٣) لجميع $x \in k$: $\psi(x) = \varphi(x)$

<u>البرهان</u> : لأن g غير قابل للتبسيط فإنه يوجد أيزومورفيزم $\hat{\varphi}: k(a) \to k'(a')$ بحيث يكون $\hat{\varphi}(x) = x$ لجميع $x \in k$ ، $\hat{\varphi}(a) = a'$ (انظر (١-٨-٣)) . ولأن $K \supset k(a)$حقل تشقيق لـــ f ، $K' \supset k(a')$ حقل تشقيق لـــ f' فإنه من (١-٨-٦) يوجد أيزومورفيزم$\psi: K \to K'$ بحيث يكون $\psi(x) = \hat{\varphi}(x)$ لجميع $x \in k(a)$ ، يرسم مجموعة أصفار f فى K على مجموعة أصفار f' فى K' .

والآن نستطيع أن نبرهن نظرية وجود ووحدانية حقول التشقيق .

<u>١-٨-٨ نظرية</u> :

ليكن k حقلاً ، f كثيرة حدود غير ثابتة فى $k[X]$. عندئذ فإن :

(١) يوجد حقل تشقيق لـــ f . إذا كان $K \supset k$ امتداد حقل ، f تتشقق على K فى عوامل خطية $X - a_1$ ، ... ، $X - a_n$ ، فإن $k(a_1, ..., a_n) \supset k$ هو حقل تشقيق لـــ f .

(٢) إذا كان $K \supset k$ ، $K' \supset k$ حقلى تشقيق لـــ f ، فإنه يوجد أيزومورفيزم $\psi: K \to K'$ بحيث يكون $\psi | k = 1$ ، يرسم مجموعة أصفار f فى K على مجموعة أصفار f فى K' . (نستطيع الآن أن نتكلم عن حقل التشقيق لكثيرة حدود غير ثابتة) .

(٣) كل حق تشقيق $K \supset k$ لـــ f يكون امتداد حقل منتهياً .

<u>البرهان</u> :

(١) باستخدام (١-٧-١) عدداً منتهياً من المرات نحصل على امتداد حقل $K \supset k$ ، $a_1, ..., a_n \in K$ ، $b \in k$ بحيث يكون :

$f = b(X - a_1)...(X - a_n)$. وهكذا تتشقق f على $k(a_1, ..., a_n)$ في عوامل خطية .

امتداد الحقل $k(a_1, ..., a_n) \supset k$ هو حقل تشقيق لـــ f ، لأنه إذا تشققت f على حقل بينى L فى الامتداد $k(a_1, ..., a_n) \supset k$ فى عوامل خطية ، فإنه يوجد $b_1, ..., b_m \in L$ ، $c \in k$ بحيث يكون $f = c(X - b_1)...(X - b_m)$. ولأن

$k(a_1,...,a_n)[X]$ نطاق تحليل وحيد ينتج أن $n=m$ ، $\{b_1,...,b_m\}=\{a_1,...,a_n\}$ ،

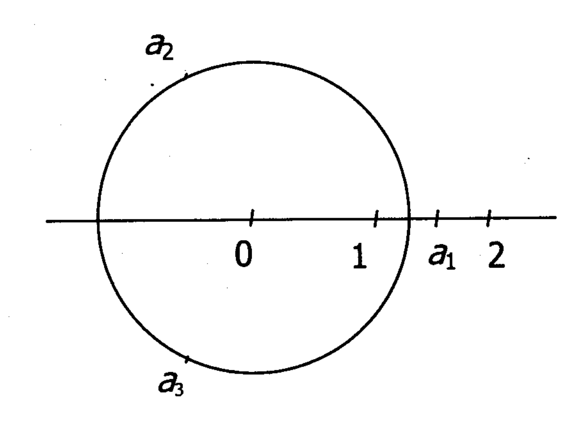
ولأن $k(b_1,...,b_m)\subset L\subset k(a_1,...,a_n)$ فإن $L=k(a_1,...,a_n)$

(٢) فى (١-٨-٦) ضع $k=k'$ ، $\varphi=1_k$ ينتج المطلوب مباشرة .

(٣) حقل التشقيق لـ f المنشأ فى (١) من (١-٦-٢) يكون منتهياً . ومن (٢) فإن كل حقل تشقيق يكون منتهياً .

١-٨-٩ مثال :

الأعداد المركبة $a_1=\sqrt[3]{2}$ ،



$$a_2=\sqrt[3]{2}(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}),$$

$$a_3=\sqrt[3]{2}(\cos\frac{4\pi}{3}+i\sin\frac{4\pi}{3})$$

هى أصفار كثيرة الحدود $f=X^3-2\in\mathbb{Q}[X]$ فى $\mathbb{C}$

ومن ثم فإن $\mathbb{Q}(a_1,a_2,a_3)$ هو حقل التشقيق لـ f ومن (١-٥-٥) يكون $\{1,a_i,a_i^2\}$ أساساً للفراغ الخطى $\mathbb{Q}(a_i)$ على $\mathbb{Q}$ ومن (١-٨-٣) يكون الراسمان

$$\mathbb{Q}(a_1)\to\mathbb{Q}(a_j),b_0+b_1a_1+b_2a_1^2\mapsto b_0+b_1a_j+b_2a_j^2,j\in\{2,3\}$$

أيزومورفيزمين

ولكل $j\neq\ell$ يكون $\mathbb{Q}(a_j)\cap\mathbb{Q}(a_\ell)=\mathbb{Q}$. لأنه لكل $x\in\mathbb{Q}(a_j)\cap\mathbb{Q}(a_\ell)$ يوجد $a,b,c,a',b',c'\in\mathbb{Q}$ بحيث إن : $a+ba_j+ca_j^2=x=a'+b'a_\ell+c'a_\ell^2$

إذا أخذنا $j=2$ ، $\ell=3$ فإننا نحصل على :

$$a+b\sqrt[3]{2}(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3})+c\sqrt[3]{4}(\cos\frac{4\pi}{3}+i\sin\frac{4\pi}{3})$$

$$=a'+b'\sqrt[3]{2}(\cos\frac{4\pi}{3}+i\sin\frac{4\pi}{3})+c'\sqrt[3]{4}(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3})$$

ومساواة الجزءين الحقيقيين فى الطرفين نحصل على :

$$a+b\sqrt[3]{2}(-\frac{1}{2})+c\sqrt[3]{4}(-\frac{1}{2})=a'+b'\sqrt[3]{2}(-\frac{1}{2})+c'\sqrt[3]{4}(-\frac{1}{2})$$

$$\Rightarrow a=a',b=b',c=c' \qquad (1)$$

وبمساواة الجزءين التخيليين نحصل على :

$$b\sqrt[3]{2}(\frac{\sqrt{3}}{2})+c\sqrt[3]{4}(-\frac{\sqrt{3}}{2})=b'\sqrt[3]{2}(-\frac{\sqrt{3}}{2})+c'\sqrt[3]{4}(\frac{\sqrt{3}}{2})$$

$$\Rightarrow b=-b',c=-c' \qquad (2)$$

من (1) ، (2) ينتج أن $b=c=0$ ، أى أن $x\in\mathbb{Q}$

وبالمثل إذا أخذنا $j=1$ ، $\ell=2$ وكذا $j=1$ ، $\ell=3$ ، فيكون $x\in\mathbb{Q}$.

أمثلة متنوعة

مثال ١ : حدد : أى التقارير الآتية صحيح وأيها خاطئ :

(أ) العدد π متسام على $\mathbb{Q}$

(ب) $\mathbb{C}$ امتداد بسيط لـــ $\mathbb{R}$

(جـ) كل عنصر فى حقل F يكون جبريا على F

(د) $\mathbb{R}$ امتداد حقل لـ $\mathbb{Q}$

(هـ) $\mathbb{Q}$ امتداد حقل لــ $\mathbb{Z}_2$

(و) ليكن $\alpha \in \mathbb{C}$ جبريا على $\mathbb{Q}$ من درجة n . إذا كان $f(\alpha)=0$ لكثيرة الحدود $0 \neq f(X) \in \mathbb{Q}[X]$ ، عندئذ فإن $\deg(f(X)) \geq n$

(ز) ليكن $\alpha \in \mathbb{C}$ جبريا على $\mathbb{Q}$ من درجة n . إذا كان $f(\alpha)=0$ لكثيرة الحدود $0 \neq f(X) \in \mathbb{R}[X]$ ، عندئذ فإن $\deg(f(X)) \geq n$

(ح) كل كثيرة حدود غير ثابتة فى $F[X]$ لها صفر فى امتداد ما للحقل F

(ط) كل كثيرة حدود غير ثابتة فى $F[X]$ لها صفر فى كل امتداد للحقل F

(ى) إذا كان X غير محدد ، فإن $\mathbb{Q}(\pi) \cong \mathbb{Q}[X]$

(ك) i جبرى على $\mathbb{Q}$

الحـــل :

(أ) ، (ب) صحيحان

(جـ) صحيح : إذا كان $a \in F$ فإن a صفر لكثيرة الحدود $X-a$

(د) صحيح

(هـ) خاطئ:العناصر فى $\mathbb{Z}_2$ ليست هى عناصر فى $\mathbb{Q}$والعمليات مختلفة كذلك فى الحقلين

(و) صحيح

(ز) خاطئ : $\sqrt{2}$ جبرى على $\mathbb{Q}$ من درجة 2 بتعريف f :

$f:=X^2-2$ ، بينما $\sqrt{2}$ جبرى على $\mathbb{R}$ من درجة 1 بتعريف f : $f:=X-\sqrt{2}$

(ح) صحيح

(ط) خاطئ : $f:=X^4+1\in\mathbb{Q}[X]$ ليس لها أصفار فى $\mathbb{R}$

(ى) صحيح

(ك) صحيح : نعرف $f:=X^2+1$ (درجة i هى 2)

<u>مثال ٢</u> : برهن على أن العدد الحقيقى $\sqrt{1+\sqrt{5}}$ جبرى على $\mathbb{Q}$

<u>البرهان</u> : ضع $c:=\sqrt{1+\sqrt{5}}$ هذا يقتضى أن $c^2=1+\sqrt{5}$ أى أن $(c^2-1)^2=5$ ، ومن ثم فإن $c^4-2c^2-4=0$. إذن نعرف كثيرة الحدود $f:=X^4-2X^2-4$ فيكون $\sqrt{1+\sqrt{5}}$ صفراً لها ، وينتج المطلوب . (العدد جبرى على $\mathbb{Q}$ من الدرجة الرابعة)

<u>مثال ٣</u> : اوجد كثيرة الحدود الصغرى من العنصر $\sqrt{1+\sqrt{5}}$ على $\mathbb{Q}$

<u>الحل</u> : مما سبق وجدنا أن $\sqrt{1+\sqrt{5}}$ صفر لكثيرة الحدود $f:=X^4-2X^2-4$ وهى كثيرة حدود مطبعة (معامل X^4 هو الواحد) . كذلك هى غير قابلة للتحليل أو التبسيط فى $\mathbb{Q}[X]$ (اختبر ذلك) . إذن فهى كثيرة الحدود الصغرى المطلوبة .

<u>مثال ٤</u> : صنف كلاً من $\alpha\in\mathbb{C}$ الآتية إذا كانت جبرية أو متسامية على <u>الحقل ***F*** المعطى</u> . إذا كانت جبرية فاوجد الدرجة .

(أ) $\alpha:=1+i\ ,\ F:=\mathbb{R}$

(ب) $\alpha:=\sqrt{\pi}\ ,\ F:=\mathbb{R}$

(جـ) $\alpha:=\sqrt{\pi}\ ,\ F:=\mathbb{Q}$

(د) $\alpha:=\sqrt{\pi}\ ,\ F:=\mathbb{Q}(\pi)$

(هـ) $\alpha:=\sqrt{\pi}+1\ ,\ F:=\mathbb{Q}(\pi^2)$

(و) $\alpha:=\pi^2\ ,\ F:=\mathbb{Q}$

(ز) $\alpha:=\pi^2\ ,\ F:=\mathbb{Q}(\pi)$

(ح) $\alpha:=\pi^2\ ,\ F:=\mathbb{Q}(\pi^3)$

(ط) $\alpha:=\sqrt{2}+\sqrt[3]{\pi}\ ,\ F:=\mathbb{Q}(\pi)$

الحل :

(أ) $\alpha=1+i$ يقتضى أن $\alpha-1=i$ ومن ثم فإن : $\alpha^2-2\alpha+1=-1$ أى أن $\alpha^2-2\alpha+2=0$ وبالتالى فإن $\alpha=1+i$ جبرية على $\mathbb{R}$ ودرجتها 2 .

(ب) $\alpha=\sqrt{\pi}$ نعرف كثيرة الحدود $f:=X-\sqrt{\pi}\in\mathbb{R}$. α جبرية ودرجتها 1

(جـ) α متسامية

(د) $\alpha=\sqrt{\pi}$ يقتضى أن $\alpha^2=\pi$ ، ونعرف $f:=X^2-\pi\in\mathbb{Q}(\pi)$. α جبرية ودرجتها 2

(هـ) $\alpha=\sqrt{\pi}+1$ يقتضى أن $(\alpha-1)^2=\pi$ ومن ثم فإن : $(\alpha-1)^4=\pi^2$. نعرف كثيرة الحدود $f:=(X-1)^4-\pi^2\in\mathbb{Q}(\pi^2)$. α جبرية ودرجتها 4

(و) α متسامية

(ز) $\alpha=\pi^2$ يقتضى أن $\alpha-\pi^2=0$. نعرف كثيرة الحدود $f:=X-\pi^2\in\mathbb{Q}(\pi)$. α جبرية ودرجتها 1

(ح) $\alpha=\pi^2$ يقتضى أن $\alpha^3=\pi^6$. نعرف f : $f:=X^3-\pi^6\in\mathbb{Q}(\pi^3)$. إذن α جبرية ومن الدرجة الثالثة .

(ط) $\alpha=\sqrt{2}+\sqrt[3]{\pi}$ يقتضى أن $(\alpha-\sqrt{2})^3=\pi$ أى أن : $\alpha^3-3\alpha^2\sqrt{2}+3\alpha.2-2\sqrt{2}=\pi$ ومن ثم فإن : $(\alpha^3+6\alpha-\pi)^2=2(3\alpha^2+2)^2$

نعرف كثيرة الحدود :

$$f:=(X^3+6X-\pi)^2-2(3X^2+2)^2\in\mathbb{Q}(\pi)$$

فيكون α جبرية ومن الدرجة 6

ملحوظة :

لاحظ أن α ليست جبرية على الإطلاق ، ولكنها جبرية على الحقل الموضح فى كل ماسبق . وكذلك f فى كل الحالات السابقة غير قابلة للتبسيط (للتحليل) ومطبعة (وذات درجة صغرى) ووحيدة .

مثال ٥ : لكل من الأعداد الجبرية $\alpha\in\mathbb{C}$ ، اوجد كثيرة الحدود الصغرى لـــ α على $\mathbb{Q}$

(أ) $\sqrt{3-\sqrt{6}}$ (ب) $\sqrt{\frac{1}{3}+\sqrt{7}}$ (جـ) $\sqrt{2}+i$

الحل : $\alpha=\sqrt{3-\sqrt{6}}$ يقتضى أن $\alpha^2=3-\sqrt{6}$ ومن ثم فإن : $\alpha^4-6\alpha^2+3=0$. كثيرة الحدود $f:=X^4-6X^2+3$ غير قابلة للتبسيط على $\mathbb{Q}$ (مثلاً باستخدام شرط أيزينشتاين) ، وهى مطبعة ، $\sqrt{3-\sqrt{6}}$ صفر لها فهى كثيرة الحدود الصغرى المطلوبة .

(ب) $\alpha=\sqrt{\frac{1}{3}+\sqrt{7}}$ يقتضى أن $\alpha^2=\frac{1}{3}+\sqrt{7}$ ، ومن ثم فإن : $\alpha^4-\frac{2}{3}\alpha^2+\frac{1}{9}=7$ ، أى أن $\alpha^4-\frac{2}{3}\alpha^2-\frac{62}{9}=0$. نعرف f كالآتى : $f:=X^4-\frac{2}{3}X^2-\frac{62}{9}$ ، وهى مطبعة وغير قابلة للتبسيط فى $\mathbb{Q}[X]$ (اختبر ذلك) ، α صفر لها . إذن هى كثيرة الحدود الصغرى المطلوبة .

(جـ) $\alpha=\sqrt{2}+i$ يقتضى أن $\alpha-\sqrt{2}=i$ وبالتالى فإن : $\alpha^2+3=2\sqrt{2}\alpha$ ومن ثم فإن : $(\alpha^2+3)^2=8\alpha$ أى أن $\alpha^4-2\alpha^2+9=0$. كثيرة الحدود $f:=X^4-2X^2+9$ مطبعة وغير قابلة للتبسيط فى $\mathbb{Q}[X]$ (اختبر ذلك) ، α صفر لها . إذن هى كثيرة الحدود المطلوبة .

مثال ٦ : ليكن E امتداداً لحقل منته F ، حيث يتألف F من q عنصراً . وليكن $\alpha\in E$ جبرياً على F من الدرجة n . برهن على أن $F(\alpha)$ يتألف من q^n عنصراً .

البرهان : α جبرى على F وله الدرجة n معناه أن f كثيرة الحدود الصغرى من α على F لها الدرجة n . ومن النظرية (١-٥-٥) نعلم أن $[F(\alpha):F]=\deg(f)$ وبهذا يكون $[F(\alpha):F]=n$. ولكن $F(\alpha)$ فراغ خطى على الحقل F وله البعد n ، وهو يتشاكل مع F^n وبهذا يكون عدد عناصره هو q^n .

مثال ٧ : ليكن E امتداداً بسيطاً $F(\alpha)$ للحقل F ، وليكن α جبرياً على F . لتكن درجة كثيرة الحدود الصغرى من α على F هى $n \geq 1$. برهن على أن أى عنصر $\beta \in E = F(\alpha)$ يمكن التعبير عنه بطريقة وحيدة كالآتى :

$$\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

حيث جميع b_i عناصر فى F .

البرهان : نريد أن نعبر أولاً عن أى عنصر فى $F(\alpha)$.

نلاحظ أولاً أنه بالنسبة للهومومورفيزم الأساسى العادى

(The usual basic homomorphism)

φ_α ، فإن كل عنصر فى

$$F(\alpha) = \varphi_\alpha(F[X])$$

يكون على الشكل

$$\varphi_\alpha(f(X)) = f(\alpha) \qquad (*)$$

كثيرة حدود شكلية (formal polynomial) فى α ، معاملاتها فى F .

لتكن كثيرة الحدود الصغرى من α على F هى :

$$p(X) = X^n + \lambda_{n-1}X^{n-1} + \ldots + \lambda_0$$

ومن حيث إن $p(\alpha) = 0$ ، فإننا نحصل على :

$$\alpha^n = -\lambda_{n-1}\alpha^{n-1} - \ldots - \lambda_0$$

وباستخدام هذه المعادلة يمكن التعبير عن كل α^m حيث $m \geq n$ بدلالة قوى α التى هى أصغر من n. وعلى سبيل المثال :

$$\begin{aligned}\alpha^{n+1} = \alpha\alpha^n &= -\lambda_{n-1}a^n - \lambda_{n-2}\alpha^{n-1} - \ldots - \lambda_0\alpha \\ &= -\lambda_{n-1}(-\lambda_{n-1}\alpha^{n-1} - \ldots - \lambda_0) - \lambda_{n-2}\alpha^{n-1} - \ldots - \lambda_0\alpha\end{aligned}$$

والآن باستخدام هذه الملحوظة فإنه إذا كانت $\beta \in F(\alpha)$ ، فإن β يمكن التعبير عنها فى الصيغة المطلوبة :

$$\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

وليس فقط الصيغة العامة (*)

وللبرهنة على وحدانية هذه الصيغة : ليكن هناك صيغتان لـــ β كالآتى :

$$b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} = \beta = b'_0 + b'_1\alpha + \ldots + b'_{n-1}\alpha^{n-1}$$

حيث $b_i, b'_i \in F$. عندئذ فإن :

$$(b_0 - b'_0) + (b_1 - b'_1)X + \ldots + (b_{n-1} - b'_{n-1})X^{n-1} = g(X) \in F[X], g(\alpha) = 0$$

وهكذا فإن درجة $g(X)$ أقل من درجة كثيرة الحدود الصغرى من α على F ، $g(\alpha) = 0$ كما ذكرنا، و $g(X)$ مطبعة ، فلابد أن يكون $g(X) = 0$. ومن ثم فإن $b_i = b'_i$ ، وتكون الصيغة وحيدة .

هل يمكنك حل المثال بطريقة أخرى ؟ راجع نظرية (١-٥-٥) !

<u>مثال ٨</u>: كثيرة الحدود $p(X) = X^2 + X + \bar{1} \in \mathbb{Z}_2[X]$ غير قابلة للتبسيط فى $\mathbb{Z}_2[X]$ لأنه إذا كانت قابلة للتبسيط فيكون لها عامل من الدرجة الأولى فيكون لها العامل X أو العامل $X + \bar{1}$ ، ولكن $p(\bar{0}) = \bar{1} \neq \bar{0}$ ، $p(\bar{1}) = \bar{1} \neq \bar{0}$ فكلاهما لايصلح عاملاً . (انظر (٢-٢-٢) فى نظرية الحلقات) .

ونحن نعلم من النظرية(١-٧-١) أنه يوجد امتداد حقل E لـــ $\mathbb{Z}_2$ يحتوى على صفر α لـــ $X^2 + X + \bar{1}$. من مثال ٧ السابق مباشرة $\mathbb{Z}_2(\alpha)$ يتكون من العناصر $\bar{0} + \bar{0}\alpha$ ، $\bar{1} + \bar{0}\alpha$ ، $\bar{0} + \bar{1}\alpha$ ، $\bar{1} + \bar{1}\alpha$ ، أى يتكون من العناصر $\bar{0}$ ، $\bar{1}$ ، α ، $\bar{1} + \alpha$.

يترك للقارئ حساب جدولى الجمع والضرب . وعلى سبيل المثال فإن :

$$\alpha(\bar{1} + \alpha) = \alpha + \alpha^2$$

ولكن $p(\alpha)=\alpha^2+\alpha+\bar{1}=\bar{0}$ ، أى أن $\alpha^2+\alpha=-\bar{1}=\bar{1}$ أى أن $\alpha(\bar{1}+\alpha)=\bar{1}$
كذلك فإن :

$$\begin{aligned}(\bar{1}+\alpha)(\bar{1}+\alpha) &= \bar{1}+\alpha+\alpha+\alpha^2 \\ &= \bar{1}+\bar{2}\alpha+\alpha^2=\bar{1}+\alpha^2=-\bar{1}\alpha=\alpha\end{aligned}$$

ملحوظة : لم نستخدم هنا $\mathbb{C}$.

<u>مثال ٩</u> : (انظر نظرية (١-٧-١))

ليكن $k=\mathbb{R}$ ، وليكن لدينا $f=X^2+1$ ونعلم أنه ليس لها أصفار فى $\mathbb{R}$ ، وبهذا تكون غير قابلة للتبسيط فى $\mathbb{R}[X]$. وبالتالى فإن $[X^2+1]$ يكون مثالياً أعظم فى $\mathbb{R}[X]$ ، ويكون $\mathbb{R}[X]/[X^2+1]$ حقلاً . سنوحد (identify) $r\in\mathbb{R}$ مع $r+[X^2+1]$ فى $\mathbb{R}/[X^2+1]$ ، وبهذا يمكن رؤية $\mathbb{R}$ كحقل جزئى من $K:=\mathbb{R}[X]/[X^2+1]$.

لتكن $\alpha:=X+[X^2+1]=:\bar{X}$. بالحساب فى $\mathbb{R}[X]/[X^2+1]$ نجد أن :

$$\begin{aligned}\alpha^2+1 &= (X+[X^2+1])(X+[X^2+1])+1 \\ &= X^2+1+[X^2+1]=[X^2+1]=\bar{0} \quad \text{(العنصر المحايد فى } K)\end{aligned}$$

أى أن α صفر لكثيرة الحدود X^2+1 .

بالطبع فإن كثيرة الحدود X^2+1 لها الصفر "i" ، لكننا هنا ننشئ حقلاً يحتوى على الأعداد الحقيقية وصفر لكثيرة الحدود X^2+1 ينشأ من استخدام الأعداد الحقيقة فقط .

<u>مثال ١٠</u> : بالاشارة إلى مثال ٨ السابق : كثيرة الحدود $X^2+X+\bar{1}$ لها α كصفر فى $\mathbb{Z}_2(\alpha)$ ، وبهذا يجب أن تتحلل إلى عوامل خطية فى $(\mathbb{Z}_2(\alpha))[X]$. اوجد هذا التحليل .

<u>الحل</u> : سنستخدم القسمة المطولة مع مراعاة أن $\bar{0}=\alpha^2+\alpha+\bar{1}$ كالآتى :

$$\begin{array}{l|l} X-\alpha & X^2+X+\bar{1} \quad \Big| \quad X+\alpha+\bar{1} \\ & X^2-\alpha X \\ \hline & \alpha X+X+\bar{1}=(\alpha+\bar{1})X+\bar{1} \\ & \alpha X-\alpha^2+X-\alpha \\ \hline & \bar{1}+\alpha^2+\alpha=\bar{0} \end{array}$$

أى أن : $(X^2+X+\bar{1})=(X-\alpha)(X+\alpha+\bar{1})$

مثال ١١ : لتكن $f:=\bar{2}X+\bar{1}\in\mathbb{Z}_4[X]$. برهن على أن f ليس لها أية أصفار فى أية حلقة تحتوى $\mathbb{Z}_4$.

البرهان : إذا كانت α صفراً لـ f فإن : $\bar{2}\alpha+\bar{1}=\bar{0}$ (1) . كذلك ولأنه فى أية حلقة تحتوى على $\mathbb{Z}_4$ يكون $\bar{4}\alpha=\bar{0}$، فإن لدينا أيضاً : $\bar{0}\underset{(1)}{=}\bar{2}(\bar{2}\alpha+1)=\bar{4}\alpha+\bar{2}=\bar{2}$

وهذا تناقض .

مثال ١٢ : بالرجوع إلى مثال ٩ السابق α جذر لـ X^2+1 .

برهن على أن X^2+1 يمكن أن تكتب على صورة حاصل ضرب عوامل خطية .

البرهان : لدينا $\alpha=X+[X^2+1]$. وبالتالى فإن :

$$(X-\alpha)(X+\alpha)=X^2-\alpha^2=X^2-(X+[X^2+1])^2$$
$$=X^2-(X^2+[X^2+1])$$

وفى نفس الوقت لدينا $X^2+[X^2+1]=-1+[X^2+1]$

ولقد اتفقنا عل أن نوحد بين 1 - ، $-1+[X^2+1]$ ، وبهذا يكون

$$(X-\alpha)(X+\alpha)=-(-1)=X^2+1$$

مثال ١٣ : اعتبر كثيرة الحدود $f := X^2 + 1 \in \mathbb{Q}[X]$. لاحظ أن :

$X^2 + 1 = (X + i)(X - i), (i = \sqrt{-1})$ ، لكن $\mathbb{C}$ ليس هو حقل تشقيق كثيرة الحدود f ، ولكن حقل تشقيقها هو $\mathbb{Q}(i) := \{r + si \mid r, s \in \mathbb{Q}\}$

بينما كما سبق فى (١-٨-٢) فإن $\mathbb{C}$ هو حقل تشقيق f **على** $\mathbb{R}$. كذلك فإن $X^2 - 2 \in \mathbb{Q}[X]$ يمكن كتابتها على الصورة $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ أى يمكن تحليلها على $\mathbb{R}$ لكن حقل تشقيقها هو $\mathbb{Q}(\sqrt{2}) := \{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}$

مثال ١٤ : اوجد حقل التشقيق لكثيرة الحدود $f := X^4 - X^2 - 2 \in \mathbb{Q}[X]$

الحل :

$$f := X^4 - X^2 - 2 = (X^2 - 2)(X^2 + 1) \in \mathbb{Q}[X]$$

وبإيجاد أصفار كثيرة الحدود : $(X^2 - 2)(X^2 + 1)$ فإن الأصفار هى $\pm\sqrt{2}, \pm i$ وبهذا يكون حقل تشقيق f على $\mathbb{Q}$ هو

$$\mathbb{Q}(\sqrt{2}, i) := \mathbb{Q}(\sqrt{2})(i) := \{\alpha + \beta i \mid \alpha, \beta \in \mathbb{Q}(\sqrt{2})\}$$
$$= \{(a + b\sqrt{2}) + (c + d\sqrt{2})i \mid a, b, c, d \in \mathbb{Q}\}$$

مثال ١٥ : اوجد حقلى تشقيق لكثيرة الحدود $f := X^2 + X + \bar{2} \in \mathbb{Z}_3[X]$

الحل :

$$f = (X - (1 + i))(X - (1 - i))$$

وبهذا يكون أحد حقلى التشقيق لـــ f على $\mathbb{Z}_3$ هو :

$$\mathbb{Z}_3(i) := \{a + bi \mid a, b \in \mathbb{Z}_3\}$$

ولايجاد الحقل الآخر : نعلم من النظرية (١-٧-١) أن العنصر

$$\beta := X + [X^2 + X + \bar{2}] \in F = \mathbb{Z}_3[X] \Big/ [X^2 + X + \bar{2}]$$

هو أيضاً صفر لـــ f . ونحن نعلم أنه لابد أن يوجد صفر آخر لـــ f موجود فى F (لأن f من درجة 2) ، ويكون F كذلك حقل تشقيق لـــ f على $\mathbb{Z}_3$. ولايجاد الصفر الآخر نجرى القسمة المطولة الآتية حيث يكون $X-\beta$ أحد عاملى f (انظر مثال ١٠ السابق) :

$$\begin{array}{r|l} & X+(\beta+\bar{1}) \\ \hline X-\beta & X^2+X+\bar{2} \\ & X^2-\beta X \\ \hline & (\beta+1)X+\bar{2} \\ & (\beta+1)X-\beta^2-\beta \\ \hline & \beta^2+\beta+\bar{2} \end{array}$$

ومن حيث إن β أحد صفرى كثيرة الحدود f فيكون

$$\beta^2+\beta+\bar{2}=\bar{0}$$

ويكون

$$\begin{aligned} f &= (X-\beta)(X+\beta+\bar{1}) \\ &= (X-\beta)(X-\bar{2}\beta-\bar{2}), \beta = X+[X^2+X+\bar{2}] \end{aligned}$$

وفى الواقع فإنه إذا كانت $p[X]$ كثيرة حدود غير قابلة للتبسيط (للتحليل) فى $F[X]$ (أى على الحقل F) ، وكان a صفراً لـــ $p(X)$ فى امتداد ما لـــ F فإن

$$F(a) \cong F[X] / p(X)$$

وهو ما يتفق مع ما ذكرناه فى (١-٨-٨) عن وحدانية حقول التشقيق .

مثال ١٦ : اعتبر كثيرة الحدود $f := X^6 - 2 \in \mathbb{Q}[X]$. واضح (باستخدام شرط أيزينشتاين) أنها غير قابلة للتحليل فى $\mathbb{Q}[X]$. كذلك هى مطبعة ، $\sqrt[6]{2}$ صفر لها فهى كثيرة الحدود الصغرى لــ $\sqrt[6]{2}$ على $\mathbb{Q}$. بتطبيق (١-٥-٥) يتضح أن :

$$\mathbb{Q}[\sqrt[6]{2}] = \mathbb{Q}(\sqrt[6]{2}) \cong \mathbb{Q}[X]/[X^6 - 2]$$

حيث

$$\{1, 2^{1/6}, 2^{2/6}, 2^{3/6}, 2^{4/6}, 2^{5/6}\}$$

أساس للفراغ الخطى $\mathbb{Q}(\sqrt[6]{2})$ على الحقل $\mathbb{Q}$ ، أى أن :

$$\mathbb{Q}(\sqrt[6]{2}) = \{a_0 + a_1 2^{1/6} + a_2 2^{2/6} + a_3 2^{3/6} + a_4 2^{4/6} + a_5 2^{5/6} \mid a_i \in \mathbb{Q}\}$$

مثال ١٧ : صف عناصر $\mathbb{Q}(\sqrt[3]{5})$

الحل : $\sqrt[3]{5}$ جبرى على $\mathbb{Q}$ لأنه صفر لكثيرة الحدود $X^3 - 5$

ومن (١-٥-٥) يكون $\{1, 5^{1/3}, 5^{2/3}\}$ أساس للفراغ الخطى $\mathbb{Q}(\sqrt[3]{5})$ على $\mathbb{Q}$ ويكون :

$$\mathbb{Q}(\sqrt[3]{5}) = \{a_0 + a_1 5^{1/3} + a_2 5^{2/3} \mid a_i \in \mathbb{Q}\}$$

مثال ١٨ : برهن على أن $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

البرهان : "$\supset$" : واضح لأن $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ يقتضى $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$

"$\subset$" : $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ يقتضى أن

$$(\sqrt{2} + \sqrt{3})^{-1} = \frac{\sqrt{3} - \sqrt{2}}{(\sqrt{3} - \sqrt{2})(\sqrt{2} + \sqrt{3})} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

أى أن $\sqrt{3} - \sqrt{2}, \sqrt{3} + \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ وينتج مباشرة أن

$$\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}), \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

مثال ١٩ : اوجد حقل التشقيق لكثيرة الحدود X^3-1 على $\mathbb{Q}$. عبر عن إجابتك فى الشكل $\mathbb{Q}(a)$.

الحل :

$$X^3-1=(X-1)(X^2+X+1)$$
$$=(X-1)(X-(\frac{-1+\sqrt{-3}}{2}))(X-(\frac{-1-\sqrt{-3}}{2}))$$

وبهذا يكون حقل التشقيق المطلوب هو $\mathbb{Q}(\sqrt{-3})$

مثال ٢٠ : صف عناصر $\mathbb{Q}(\pi)$

الحل : π ليس عدداً جبريا على $\mathbb{Q}$ حتى تنطبق عليه النظرية (١-٥-٥) . وواضح أن

$$\mathbb{Q}(\pi)=\{\frac{a_n\pi^n+\ldots+a_1\pi+a_0}{b_m\pi^m+\ldots+b_1\pi+b_0}\,|\,a_i,b_i\in\mathbb{Q},b_m\neq 0\}$$

مثال ٢١ : اوجد كثيرة حدود $p(X)$ فى $\mathbb{Q}[X]$ بحيث يكون

$$\mathbb{Q}(\sqrt{1+\sqrt{5}})\cong \mathbb{Q}[X]/[p(X)]$$

الحل : سنحصل على كثيرة الحدود الصغرى للعنصر $\sqrt{1+\sqrt{5}}$ على $\mathbb{Q}$ ثم نطبق النظرية (١-٥-٥) كالآتى :

$$X=\sqrt{1+\sqrt{5}}\Rightarrow X^2=1+\sqrt{5}\Rightarrow (X^2-1)^2=5$$
$$\Rightarrow X^4-2X^2-4=0$$

تكون كثيرة الحدود الصغرى المطلوبة هى $p(X)=X^4-2X^2-4$

مثال ٢٢ : اوجد $a,b,c\in\mathbb{Q}$ بحيث يكون :

$$(1+\sqrt[3]{4})/(2-\sqrt[3]{2})=a+b\sqrt[3]{2}+c\sqrt[3]{4}$$

(لاحظ أن a ، b ، c موجودة لأن :

$$\frac{(1+\sqrt[3]{4})}{(2-\sqrt[3]{2})} \in \mathbb{Q}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q}\}$$

<u>**الحل**</u> : لاحظ أن $\sqrt[3]{2}$ جبرى على $\mathbb{Q}$ لأنه صفر لكثيرة الحدود الصغرى $X^3-2 \in \mathbb{Q}[X]$ وبهذا تكون $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ أساساً للفراغ الخطى $\mathbb{Q}(\sqrt[3]{2})$ على $\mathbb{Q}$.

والآن :

$$\frac{1+\sqrt[3]{4}}{2-\sqrt[3]{2}} = a+b\sqrt[3]{2}+c\sqrt[3]{4}$$

$$\Rightarrow 1+\sqrt[3]{4} = 2a+2b\sqrt[3]{2}+2c\sqrt[3]{4}-a\sqrt[3]{2}-b\sqrt[3]{4}-2c$$

ولأن $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ أساس لـ $\mathbb{Q}(\sqrt[3]{2})$ على $\mathbb{Q}$:

$$\Rightarrow \quad 2a-2c=1 \qquad (1)$$

$$2b-a=0 \qquad (2)$$

$$2c-b=1 \qquad (3)$$

من (1) ، (3) ينتج أن :

$$2a-b=2 \qquad (4)$$

من (2) ، (4) ينتج أن : $a=\frac{4}{3}$ ، $b=\frac{2}{3}$. وبالتعويض فى (3) نحصل على $c=\frac{5}{6}$

<u>**مثال ٢٣**</u> : برهن على أن $\mathbb{Q}(4-i)=\mathbb{Q}(1+i) \quad (i=\sqrt{-1})$

<u>**البرهان**</u> : سنثبت أن $4-i \in \mathbb{Q}(1+i)$ كالآتى :

$1+i,-2 \in \mathbb{Q}(1+i)$ فينتج أن $-1+i \in \mathbb{Q}(1+i)$ ، فينتج أن $1-i \in \mathbb{Q}(1+i)$.

$3 \in \mathbb{Q}(1+i)$ فينتج أن $4-i \in \mathbb{Q}(1+i)$. ونثبت بالمثل أن $1+i \in \mathbb{Q}(4-i)$ كالآتى :

$4-i, 3 \in \mathbb{Q}(4-i)$ فينتج أن $1-i \in \mathbb{Q}(4-i)$. كذلك $1 \in \mathbb{Q}(4-i)$ فينتج أن $i \in \mathbb{Q}(4-i)$ فينتج أن $1+i \in \mathbb{Q}(4-i)$.

<u>مثال ٢٤</u> : عبر عن $(3+4\sqrt{2})^{-1}$ فى الصورة $a+b\sqrt{2}$ حيث $a,b \in \mathbb{Q}$

<u>الحل</u> :

$$(3+4\sqrt{2})^{-1} = \frac{3-4\sqrt{2}}{(3+4\sqrt{2})(3-4\sqrt{2})} = \frac{3-4\sqrt{2}}{-23} = -\frac{3}{23} + \frac{4}{23}\sqrt{2}$$

<u>مثال ٢٥</u> : برهن على أن $\mathbb{Q}(\sqrt{2})$ لايتشاكل مع $\mathbb{Q}(\sqrt{3})$.

<u>البرهان</u> : ليكن $\mathbb{Q}(\sqrt{2})$ متشاكلاً مع $\mathbb{Q}(\sqrt{3})$ أى أنه يوجد تشاكل (أيزومورفيزم) φ :

$$\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$$

واضح أن $\varphi | \mathbb{Q} = 1_{\mathbb{Q}}$. كذلك فإن $\varphi(\sqrt{2}) = \sqrt{3}$. ومن ثم فإن :

$$2 = \varphi(2) = \varphi(\sqrt{2}.\sqrt{2}) = \varphi(\sqrt{2}).\varphi(\sqrt{2}) = \sqrt{3}.\sqrt{3} = 3$$

وهذا تناقض .

<u>مثال ٢٦</u> : اوجد جميع الحقول الجزئية فى $\mathbb{Q}(\sqrt{2})$

<u>الحل</u> : $\mathbb{Q}$ حقل جزئى فى $\mathbb{Q}(\sqrt{2})$ ولايوجد حقل فعلى فى $\mathbb{Q}$. إذن نبحث عن حقول بينية فى امتداد الحقل $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. ليكن هناك الحقل البينى L . نعلم من نظرية الدرجة (١-٢-٤) أن

$$[\mathbb{Q}(\sqrt{2}) : L][L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

ومن (١-٥-٥) $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ لأن $f = X^2 - 2$ هى كثيرة الحدود الصغرى من $\sqrt{2}$ على $\mathbb{Q}$. أى أن

$$[\mathbb{Q}(\sqrt{2}) : L][L : \mathbb{Q}] = 2$$

هذا معناه أن $[L:\mathbb{Q}]=1$ أو $[\mathbb{Q}(\sqrt{2}):L]=1$ أى أن $L=\mathbb{Q}$ أو $L=\mathbb{Q}(\sqrt{2})$.

مثال ٢٧:اوجد حقل تشقيق كثيرة الحدود X^n-a على $\mathbb{Q}$ حيث a عدد كسرى(نسبى) موجب

الحل : أصفار كثيرة الحدود المعطاة فى $\mathbb{Q}(\sqrt[n]{a},\omega)$ حيث $1,\omega,\dots,\omega^{n-1}$ الجذور النونية للواحد هى :

$$a^{1/n},\omega a^{1/n},\omega^2 a^{1/n},\dots,\omega^{n-1}a^{1/n}$$

ويكون $\mathbb{Q}(\sqrt[n]{a},\omega)$ هو حقل التشقيق المطلوب .

مثال ٢٨ : لقد ذكرنا بدون برهان أن π ، e متساميان على $\mathbb{Q}$

(أ) اوجد حقلاً جزئياً $F\subset\mathbb{R}$ بحيث تكون π جبرية من درجة 3 على F

(ب) اوجد حقلاً جزئياً $E\subset\mathbb{R}$ بحيث يكون $e+\pi$ جبرياً من درجة 5 على E

الحل :

(أ) واضح أننا سنبدأ من $\mathbb{Q}$ ثم نجرى عملية ضم (أو إلحاق) ، وحتى تكون π جبرية من الدرجة 3 على الحقل F فيجب أن تكون صفراً لكثيرة الحدود X^3-a جيث $a\in F$. نأخذ $a=\pi^3$ فيكون $F=\mathbb{Q}(\pi^3)$. لاحظ أن كثيرة الحدود غير قابلة للتبسيط على $\mathbb{Q}(\pi^3)$

(ب) مثل (أ) كثيرة الحدود هنا $X^5-(e+\pi)^5$ ويكون $E=\mathbb{Q}(e,\pi^5)$

مثال ٢٩ :

(أ) برهن على أن $X^3+X^2+\bar{1}$ غير قابلة للتحليل (للتبسيط) فى $\mathbb{Z}_2[X]$

(يقال كذلك كما سبق غير قابلة للتحليل (للتبسيط على $\mathbb{Z}_2$)

(ب) ليكن α صفراً لكثيرة الحدود $X^3+X^2+\bar{1}$ فى امتداد للحقل $\mathbb{Z}_2$.

برهن على أن $X^3+X^2+\bar{1}$ تتحلل إلى عوامل خطية فى $(\mathbb{Z}_2(\alpha))[X]$ بإيجاد هذه العوامل فعلياً .

<u>الحل</u> : إذا كانت $f := X^3 + X^2 + \bar{1}$ قابلة للتحليل فى $\mathbb{Z}_2[X]$ فيكون لها عامل من الدرجة الأولى أى على الشكل $X - \gamma$. ومن حيث إن $\mathbb{Z}_2$ يتكون من عنصرين فقط هما $\bar{0}$ ، $\bar{1}$ فإن γ إذا وجدت تكون $\gamma = \bar{0}$ أو $\gamma = \bar{1}$ ، ويكون $f(\bar{0}) = \bar{0}$ أو $f(\bar{1}) = \bar{0}$. نحسب $f(\bar{0})$ ، $f(\bar{1})$:

$$f(\bar{0}) = \bar{0} + \bar{0} + \bar{1} = \bar{1} \neq \bar{0},$$
$$f(\bar{1}) = \bar{1} + \bar{1} + \bar{1} = \bar{1} \neq \bar{0}$$

إذن f غير قابلة للتحليل فى $\mathbb{Z}_2[X]$ (أى غير قابلة للتحليل على $\mathbb{Z}_2$) .

(ب) سنستخدم الآن مثال ٧ السابق . $X^3 + X^2 + \bar{1}$ هى كثيرة الحدود الصغرى للعنصر α الذى يلحق (يضم) لـــ $\mathbb{Z}_2$ لتكوين $\mathbb{Z}_2(\alpha)$ حتى يمكن أن تتحلل f عليه.

وبالتالى فإن أى عنصر فى $\mathbb{Z}_2(\alpha)$ يكون على الشكل :

$$\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2, \quad \lambda_i = \bar{0}, \bar{1} \qquad (*)$$

سنقسم $X^3 + X^2 + \bar{1}$ قسمة مطولة على $X - \alpha$ كالآتى :

$$\begin{array}{r|l}
 & X^2 + (\alpha + \bar{1})X + (\alpha^2 + \alpha) \\
X - \alpha & X^3 + X^2 + \bar{1} \\
 & \underline{X^3 - \alpha X^2} \\
 & (\alpha + 1)X^2 + \bar{1} \\
 & \underline{(\alpha + 1)X^2 - (\alpha^2 + \alpha)X} \\
 & (\alpha^2 + \alpha)X + \bar{1} \\
 & \underline{(\alpha^2 + \alpha)X - \alpha^3 - \alpha^2} \\
 & \alpha^3 + \alpha^2 + \bar{1} = \bar{0}
\end{array}$$

$\bar{\alpha}^3+\alpha^2+\bar{1}=\bar{0}$ لأن α صفر لـ $f=\chi^3+\chi^3+1$ فى $\mathbb{Z}_2(\alpha)$

والآن نحصل على العامل الخطى الأول فى خارج القسمة $g:=X^2+(\alpha+1)X+(\alpha^2+\alpha)$

وسنستخدم هذه المرة تجربة العناصر الثمانية فى $\mathbb{Z}_2(\alpha)$ (انظر *) وهى :

$\bar{0}$ ، $\bar{1}$ ، α ، α^2 ، $\bar{1}+\alpha$ ، $\bar{1}+\alpha^2$ ، $\alpha+\alpha^2$ ، $\bar{1}+\alpha+\alpha^2$. وبتجربة α^2 نحصل على :

$$\alpha^4+(\alpha+1)\alpha^2+\alpha^2+\alpha=\alpha^4+\alpha^3+\bar{2}\alpha^2+\alpha$$
$$\underset{(\bar{2}=\bar{0})}{=}\alpha^4+\alpha^3+\alpha=\bar{0}$$

أى أن $X-\alpha^2$ عامل خطى لـ $X^3+X^2+\bar{1}$.

ومن حيث إن $X^3+X^2+\bar{1}$ كثيرة حدود من الدرجة الثالثة ، يتبقى عامل أخير . نفضل أن نحصل عليه بالقسمة المطولة مرة أخرى لخارج القسمة $X^2+(\alpha+\bar{1})X+(\alpha^2+\alpha)$ على $X-\alpha^2$ كالآتى :

$$\begin{array}{r|l} & X+\alpha^2+\alpha+\bar{1} \\ X-\alpha^2 & X^2+(\alpha+\bar{1})X+\alpha^2+\alpha \\ & X^2-\alpha^2X \\ \hline & (\alpha^2+\alpha+\bar{1})X+\alpha^2+\alpha \\ & (\alpha^2+\alpha+\bar{1})X-\alpha^4-\alpha^3-\alpha^2 \\ \hline & \alpha^4+\alpha^3+\bar{2}\alpha^2+\alpha=\alpha^4+\alpha^3+\alpha \end{array}$$

(لاحظ أن $\bar{2}=\bar{0}$ فى $\mathbb{Z}_2$)

باقى القسمة هو $\alpha^4+\alpha^3+\alpha$ وهو يساوى $\alpha(\alpha^3+\alpha^2+\bar{1})=\bar{0}$ كما سبق .

إذن تتحلل $X^3+X^2+\bar{1}$ على $\mathbb{Z}_2(\alpha)$ كالآتى :

$$X^3+X^2+\bar{1}=(X-\alpha)(X-\alpha^2)(X-(\alpha^2+\alpha+\bar{1}))$$

(لاحظ أن $\alpha^2+\alpha+\bar{1}=-(\alpha^2+\alpha+\bar{1})$ فى $\mathbb{Z}_2(\alpha)$)

مثال ٣٠ : ما درجة الامتدادين : $\mathbb{C}\supset\mathbb{R}$ ، $\mathbb{C}\supset\mathbb{Q}$

الحل : $[\mathbb{C}:\mathbb{R}]=2$ أى أن درجة الامتداد $\mathbb{C}\supset\mathbb{R}$ هى 2 ، لأن $\{1, i\}$ يصلح أساساً للفراغ الخطى $\mathbb{C}$ على $\mathbb{R}$. بينما $[\mathbb{C}:\mathbb{Q}]=\infty$.

مثال ٣١ : اوجد $[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}]$

الحل :

$$\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=(\mathbb{Q}(\sqrt{2}))(\sqrt[3]{2})$$

وبالتالى فإن

$$[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}]=[(\mathbb{Q}(\sqrt{2}))(\sqrt[3]{2}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$$

$$=\deg(X^3-2)\deg(X^2-2)$$ (انظر (١-٥-٥)

$$=3.2\ =6$$

ومن مثال٦ $[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}]=6$

(أى أن $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})\cong\mathbb{Q}(\sqrt[6]{2})$ بل $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=\mathbb{Q}(\sqrt[6]{2})$ لأن $\mathbb{Q}(\sqrt[6]{2})$ ، $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$ لهما نفس الأساس كفراغين خطيين على الحقل $\mathbb{Q}$. وفى الواقع فإنه من الواضح تماماً أن $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})\supset\mathbb{Q}(\sqrt[6]{2})$)

ملحوظة : يمكن أن نبرهن على أن $\mathbb{Q}(\sqrt[6]{2})=\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$ كذلك بملاحظة أن :

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt[6]{2})\subset\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$$

$$\Rightarrow 6=[\mathbb{Q}\sqrt{2},\sqrt[3]{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt[6]{2})].[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}]$$

$$=[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt[6]{2})].6$$

$$\Rightarrow[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt[6]{2})]=1$$

وبصفة عامة إذا كان E امتداداً لـ F (كحلقين) وكان $[E: F] = 1$ فإن $E=F(1)=F$

مثال ٣٢ : اوجد $[\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}]$

الحل : كما سبق فى مثال ٣١ $\mathbb{Q}(\sqrt{3},\sqrt{5}) = (\mathbb{Q}(\sqrt{3}))(\sqrt{5})$

ومن ثم فإن :

$$[\mathbb{Q}\sqrt{3},\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3}))(\sqrt{5}):\mathbb{Q}(\sqrt{3})].[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$$

$$\underset{5-5-1}{=} \deg(X^2-5).\deg(X^2-3)$$

$$= 2.2 = 4$$

طريقة أخرى : $\{1,\sqrt{3}\}$ أساس للفراغ الخطى $\mathbb{Q}(\sqrt{3},\sqrt{5})$ على الحقل $\mathbb{Q}(\sqrt{5})$ ، $\{1,\sqrt{5}\}$ أساس للفراغ الخطى $\mathbb{Q}(\sqrt{5})$ على الحقل $\mathbb{Q}$

ومن برهان نظرية الدرجة يكون $\{1,\sqrt{3},\sqrt{5},\sqrt{3}\sqrt{5}\}$ أى $\{1,\sqrt{3},\sqrt{5},\sqrt{15}\}$ أساساً للفراغ الخطى $\mathbb{Q}(\sqrt{3},\sqrt{5})$ على الحقل $\mathbb{Q}$.

مثال ٣٣ : اوجد كثيرة الحدود الصغرى للعنصر $\sqrt{-3}+\sqrt{2}$ على $\mathbb{Q}$

الحل : ضع $X = \sqrt{-3}+\sqrt{2}$. هذا يقتضى أن

$$X^2 = -3+2+2\sqrt{-6} = -1+2\sqrt{-6}$$

أى أن $X^2+1 = 2\sqrt{-6}$. وبالتالى فإن : $X^4+2X^2+1=-24$

ومن ثم فإن : X^4+2X^2+25 هى كثيرة الحدود الصغرى المطلوبة .

لاحظ أن $\sqrt{-3}+\sqrt{2}$ صفر لها ، وهى مطبعة ، وهى غير قابلة للتبسيط على $\mathbb{Q}$.

مثال ٣٤ : ليكن E امتداداً منتهياً للحقل $\mathbb{R}$. برهن على أن $E=\mathbb{R}$ أو $E=\mathbb{C}$

البرهان : الحقل E امتداد منته للحقل $\mathbb{R}$ فينتج أن E امتداد جبرى للحقل $\mathbb{R}$ (انظر (١-٦-٢)). وبالتالى فإن $\mathbb{C} \subset E$. ولكن :

(من نظرية الدرجة) $2 = [\mathbb{C}:\mathbb{R}] = [\mathbb{C}:E][E:\mathbb{R}]$

أى أن $2=[\mathbb{C}:E]$ أو $[\mathbb{C}:E]=1$

$[\mathbb{C}:E]=2$ يقتضى أن $E=\mathbb{R}$ ، $[\mathbb{C}:E]=1$ يقتضى أن $E=\mathbb{C}$.

مثال ٣٥ : ليكن $a,b\in\mathbb{Q}$ ، $b\neq 0$. برهن على أن $\mathbb{Q}(\sqrt{a})=\mathbb{Q}(\sqrt{b})$ يستلزم أنه يوجد $c\in\mathbb{Q}$ بحيث يكون $a=bc^2$.

البرهان : لدينا حالتان : الحالة الأولى : $\sqrt{b}\in\mathbb{Q}$. وبالتالى فإن $\sqrt{a}\in\mathbb{Q}$. نعرف $c:=\frac{\sqrt{a}}{\sqrt{b}}\in\mathbb{Q}$ أى أن $a=c^2b$.

الحالة الثانية : $\sqrt{b}\notin\mathbb{Q}$: وبالتالى فإن $\sqrt{a}\notin\mathbb{Q}$. ضع $\sqrt{a}=x+y\sqrt{b}\in\mathbb{Q}(\sqrt{b})$ فينتج أن $x=0$ ومن ثم فإن $a=by^2$.

مثال ٣٦ : لتكن $f:=aX^2+bX+c\in\mathbb{Q}[X]$. اوجد عنصراً بدائياً (انظر (١-٣-٣)) لحقل التشقيق لـــ f على $\mathbb{Q}$

الحل : إذا كان α صفراً لـــ f فإن : $a=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$

وبالتالى فإن العنصر البدائى $\sqrt{b^2-4ac}$ يجعل $\mathbb{Q}(\sqrt{b^2-4ac})$ حقل تشقيق لـــ f على $\mathbb{Q}$.

مثال ٣٧ : ليكن E امتداداً للحقل F ، $\alpha\in E$ جبرياً على F ، $\beta\in F(\alpha)$. برهن على أن درجة β تقسم درجة α .

الحل : درجة α هى درجة كثيرة الحدود الصغرى من العنصر α على الحقل F (راجع (١-٤-١)،(١-٥-٣))، وبالطبع كذلك بالنسبة إلى β . كذلك لدينا من (١-٥-٥) : درجة كثيرة الحدود الصغرى من α بالنسبة إلى الحقل F هى : $[F(\alpha):F]$ (وبالمثل بالنسبة إلى β) . والآن

(لأن $\beta\in F(\alpha)$) $\quad F\subset F(\beta)\subset F(\alpha)$

(نظرية الدرجة) $\quad \Rightarrow [F(\alpha):F]=[F(\alpha):F(\beta)].[F(\beta):F]$

أى أن درجة β تقسم درجة α .

مثال ٣٨ :برهن على أنه لايوجد عنصر فى $\mathbb{Q}(\sqrt{2})$ يكون صفراً لكثيرة الحدود X^3-2

البرهان : أى صفر لكثيرة الحدود X^3-2 ستكون كثيرة الحدود هذه بالنسبة له هى كثيرة الحدود الصغرى على $\mathbb{Q}$ ، ودرجته هى درجتها 3 . بينما لايوجد أى عنصر فى $\mathbb{Q}(\sqrt{2})$ درجته 3 ، لأنه لايوجد أى عنصر فى $\mathbb{Q}(\sqrt{2})$ تكون كثيرة الحدود الصغرى له على $\mathbb{Q}$ درجتها 3 .

مثال ٣٩ : برهن على أن $\mathbb{Q}(\sqrt{3}+\sqrt{7})=\mathbb{Q}(\sqrt{3},\sqrt{7})$

البرهان : $\sqrt{3},\sqrt{7}\in\mathbb{Q}(\sqrt{3},\sqrt{7})$ يقتضى أن $\sqrt{3}+\sqrt{7}\in\mathbb{Q}(\sqrt{3},\sqrt{7})$ أى أن $\mathbb{Q}(\sqrt{3}+\sqrt{7})\subset\mathbb{Q}(\sqrt{3},\sqrt{7})$. (1)

والآن $\sqrt{3}+\sqrt{7}\in\mathbb{Q}(\sqrt{3},\sqrt{7})$ يقتضى أن

$$(\sqrt{3}+\sqrt{7})^{-1}=\frac{\sqrt{7}-\sqrt{3}}{(\sqrt{7}+\sqrt{3})(\sqrt{7}-\sqrt{3})}\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$$

أى أن $\frac{\sqrt{7}-\sqrt{3}}{4}\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$ ومن ثم فإن : $\sqrt{7}-\sqrt{3}\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$

ولكن $\sqrt{3}+\sqrt{7}\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$ ، وبالتالى فإن $\sqrt{3},\sqrt{7}\in\mathbb{Q}(\sqrt{3}+\sqrt{7})$ أى أن $\mathbb{Q}(\sqrt{3},\sqrt{7})\subset\mathbb{Q}(\sqrt{3}+\sqrt{7})$ (2) . من (1) ، (2) ينتج المطلوب مباشرة .

مثال ٤٠ : اوجد درجة كل من الامتدادين الآتيين وأساساً لكل منهما :

(أ) $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$ على $\mathbb{Q}$

(ب) $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ على $\mathbb{Q}$

الحل :

(أ) $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})=(\mathbb{Q}(\sqrt[3]{2}))(\sqrt{3})$

وبالتالى فمن نظرية الدرجة :

$$[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}]=[(\mathbb{Q}(\sqrt{3}))(\sqrt[3]{2}):\mathbb{Q}(\sqrt{3})].[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$$
$$=\deg(X^3-2).\deg(X^2-2)=3.2=6$$

سنتخذ $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ أساساً للامتداد $\mathbb{Q}(\sqrt{3})(\sqrt[3]{2})\supset\mathbb{Q}(\sqrt{3})$ ، $\{1,\sqrt{3}\}$ أساساً للامتداد $\mathbb{Q}(\sqrt{3})\supset\mathbb{Q}$ (انظر (١-٥-٥)) ، ومن ثم سنتخذ

$$\{1,\sqrt{3},\sqrt[3]{2},\sqrt[3]{2}\sqrt{3},\sqrt[3]{4},\sqrt[3]{4}\sqrt{3}\}$$

أساساً للامتداد $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})\supset\mathbb{Q}$ (انظر برهان نظرية الدرجة)

(ب) $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})=((\mathbb{Q}(\sqrt{2}))(\sqrt{3}))(\sqrt{5})$

وبالتالى فمن نظرية الدرجة

$$[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}] \overset{\text{نظرية الدرجة}}{=} [\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{3})].[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})].[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$$

$$=\deg(X^2-5).\deg(X^2-3).\deg(X^2-2)=2.2.2=8$$

سنتخذ $\{1,\sqrt{5}\}$ أساساً للامتداد $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})\supset\mathbb{Q}(\sqrt{2},\sqrt{3})$ ، $\{1,\sqrt{3}\}$ أساساً للامتداد $\mathbb{Q}(\sqrt{2},\sqrt{3})\supset\mathbb{Q}(\sqrt{2})$ ، $\{1,\sqrt{2}\}$ أساساً للامتداد $\mathbb{Q}(\sqrt{2})\supset\mathbb{Q}$. ومن ثم (كما سبق) نتخذ

$$\{1,\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{2}\sqrt{3},\sqrt{2}\sqrt{5},\sqrt{3}\sqrt{5},\sqrt{2}\sqrt{3}\sqrt{5}\}$$

أساساً للامتداد $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})\supset\mathbb{Q}$

<u>مثال ٤١</u> : اوجد درجة كل من امتدادات الحقول الآتية ، واوجد أساساً فى كل حالة :

(أ) $\mathbb{Q}(\sqrt{2},\sqrt{6})\supset\mathbb{Q}(\sqrt{3})$ (ب) $\mathbb{Q}(\sqrt{2}+\sqrt{3})\supset\mathbb{Q}(\sqrt{3})$

(جـ) $\mathbb{Q}(\sqrt{2},\sqrt{3})\supset\mathbb{Q}(\sqrt{2}+\sqrt{3})$ (د) $\mathbb{Q}(\sqrt{2},\sqrt{6}+\sqrt{10})\supset\mathbb{Q}(\sqrt{3}+\sqrt{5})$

<u>الحل</u> : (أ)

$$[\mathbb{Q}(\sqrt{2},\sqrt{6}):\mathbb{Q}(\sqrt{3})]=[\mathbb{Q}(\sqrt{2},\sqrt{2}\sqrt{3}):\mathbb{Q}(\sqrt{3})]$$
$$=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{3})]=\deg(X^2-2)=2$$

سنتخذ الأساس $\{1,\sqrt{2}\}$

(ب)

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{3})] \quad = \quad [(\mathbb{Q}(\sqrt{3}))(\sqrt{2}):\mathbb{Q}(\sqrt{3})]$$

مثال ١٨

$$= \deg(X^2-2) = 2$$

سنتخذ الأساس $\{1,\sqrt{2}\}$

(جـ) $$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3})] \quad = \quad [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2},\sqrt{3})]=1$$

مثال ١٨

وسنتخذ الأساس $\{1\}$

(د) $$[\mathbb{Q}(\sqrt{2},\sqrt{6}+\sqrt{10}):\mathbb{Q}(\sqrt{3}+\sqrt{5})]$$

$$=[\mathbb{Q}(\sqrt{2},\sqrt{2}(\sqrt{3}+\sqrt{5})):\mathbb{Q}(\sqrt{3}+\sqrt{5})]=[\mathbb{Q}(\sqrt{2},\sqrt{3}+\sqrt{5}):\mathbb{Q}(\sqrt{3}+\sqrt{5})]$$
$$=[(\mathbb{Q}(\sqrt{3}+\sqrt{5}))(\sqrt{2}):\mathbb{Q}(\sqrt{3}+\sqrt{5})]$$
$$=\deg(X^2-2)=2$$

سنتخذ الأساس $\{1,\sqrt{2}\}$

<u>مثال ٤٢</u> : حدد : أى التقارير الآتية صحيح وأيها خاطئ

(١) كل امتداد حقل منته يكون امتداداً جبرياً

(٢) كل امتداد جبرى لحقل يكون امتداداً منتهياً

(٣) الحقل "القمة" "لبرج" منته من امتدادات منتهية لحقول يكون امتداداً منتهياً للحقل"القاع"

(إذا كان لدينا "عمود" من الحقول كل حقل يحتوى على الحقل الذى يسبقه مباشرة فإنه

يقال إن لدينا "برجاً" (tower) من الحقول . مثال ذلك ($\begin{matrix}\mathbb{C}\\|\\\mathbb{R}\\|\\\mathbb{Q}\end{matrix}$)

(٤) $\mathbb{R}$ مغلقة جبريا

(يقال لحقل F إنه **مغلق جبرياً** (algebraically closed) إذا كانت كل كثيرة حدود غير ثابتة فى $F[X]$ لها صفر فى F)

(٥) $\mathbb{Q}$ مغلقة جبريا داخل $\mathbb{R}$

(٦) $\mathbb{C}$ مغلقة جبريا داخل $\mathbb{C}(X)$ ، حيث X غير محددة

(٧) $\mathbb{C}(X)$ مغلقة جبريا ، حيث X غير محددة

(٨) الحقل $\mathbb{C}(X)$ ليس له **إغلاق جبرى** (algebraic closure) ، لأن $\mathbb{C}$ تحتوى جميع الأعداد الجبرية

(ليكن E امتداداً للحقل F . عندئذ فإن :

$$\overline{F}_E := \{\alpha \in E \mid \alpha \text{ جبرى على } F\}$$

هو حقل جزئى من E ، يسمى **الإغلاق الجبرى** لـــ F فى E)

(٩) مميز أى حقل مغلق جبرياً يساوى الصفر

(١٠) إذا كان E امتداداً مغلقا جبريا للحقل F ، فإن E يكون امتداداً جبريا لـــ F

الحل : (١) ، (٣) ، (٦) صحيحة . والباقى خاطئ .

مثال ٤٣ : الحقل $\overline{\mathbb{Q}}$: حقل جميع الأعداد المركبة الجبرية على $\mathbb{Q}$ (تسمى باختصار **الأعداد الجبرية**) مغلق جبرياً

$\mathbb{C}$ إغلاق جبرى على $\mathbb{R}$ ، لكن $\mathbb{C}$ ليست إغلاقاً جبرياً على $\mathbb{Q}$ ، لأنه توجد أعداد متسامية

الحقل $\overline{\mathbb{Q}}$ إغلاق جبرى لـــ $\mathbb{Q}$

مثال ٤٤ : برهن على أن الحقل F يكون مغلقاً جبرياً إذا كانت وفقط إذا كانت كل كثيرة حدود غير ثابتة فى $F[X]$ تتحلل إلى عوامل خطية .

البرهان : ليكن الحقل F مغلقاً جبريا . ولتكن f كثيرة حدود غير ثابتة فى $F[X]$. عندئذ فإن f لها صفر $a \in F$. ومن (٢-٢-٢) فى نظرية الحلقات يكون $X - a$ عاملاً لـــ f ، بحيث يكون $f = (X-a)g$. عندئذ إذا كانت g ليست ثابتة فيكون لها صفر $b \in F$ ، ويكون $f = (X-a)(X-b)h$. وبالاستمرار بهذه الطريقة نحصل على تحليل لـــ f فى صورة عوامل خطية .

وبالعكس ، لتكن كل كثيرة حدود غير ثابتة في $F[X]$ لها تحليل في صورة عوامل خطية . إذا كان $aX - b$ عاملاً خطياً لـــ f ، فإن b/a يكون صفراً لـــ f . وهكذا يكون F مغلقاً جبرياً .

مثال ٤٥ : برهن على أن أى حقل مغلق جبرياً لايكون له امتدادات جبرية فعلية ، أى أنه لاتوجد امتدادات جبرية E بحيث يكون $F \subsetneq E$

البرهان : ليكن E امتداداً جبرياً لـــ F ، بحيث يكون $F \subset E$. عندئذ إذا كان $\alpha \in E$ ، فلدينا من مثال ٤٤ السابق مباشرة ، كثيرة الحدود الصغرى لـــ α على $F: f = X - \alpha$ (لأن F مغلق جبرياً) ، وهكذا فإن $\alpha \in F$ ، وبالتالى فإن $E = F$.

مثال ٤٦ : لتكن $f \in F[X]$. إذا كانت a تنتمى إلى امتداد ما لـــ F ، $f(a)$ جبرية على F . برهن على أن a جبرية على F .

البرهان : $f(a)$ جبرية على F تقتضى وجود $g \in F[X]$ بحيث إن $g(f(a)) = 0$ وهذا معناه أنه $(gof)(a) = 0$ حيث $gof \in F[X]$ أى أن a جبرية على F .

مثال ٤٧ : برهن على أن $X^2 - 3$ غير قابلة للتحليل (للتبسيط) على $\mathbb{Q}(\sqrt[3]{2})$

البرهان : أى عنصر فى $\mathbb{Q}(\sqrt[3]{2})$ يكون على الصورة $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ حيث $a,b,c \in \mathbb{Q}$ (انظر مثال ٧ ونظرية (١-٥-٥) حيث $X^3 - 2$ هى كثيرة الحدود الصغرى للعنصر $\sqrt[3]{2}$ على $\mathbb{Q}$) . وإذا كانت $X^2 - 3$ قابلة للتبسيط (للتحليل) على $\mathbb{Q}(\sqrt[3]{2})$ فإنه يكون لها صفر فى الحقل $\mathbb{Q}(\sqrt[3]{2})$ أى أنه يوجد $a,b,c \in \mathbb{Q}$ بحيث يكون :

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})^2 - 3 = 0$$

أى أن :

$$a^2 + 4bc + (2c^2 + 2ab)2^{1/3} + (b^2 + 2ac)2^{2/3} = 3$$

ومن حيث إن $\{1, 2^{1/3}, 2^{2/3}\}$ أساس للفراغ الخطى $\mathbb{Q}(\sqrt[3]{2})$ على $\mathbb{Q}$ ، فإن :

$$a^2 + 4bc = 3, \qquad (1)$$

$$c^2 + ab = 0, \qquad (2)$$

$$b^2 + 2ac = 0 \qquad (3)$$

من (2) نحصل على (4) $a = -\dfrac{c^2}{b}$ حيث $b \neq 0$. ($b = 0$ يقتضى أن $a = \pm\sqrt{3}$

وهذا تناقض لأن $a \in \mathbb{Q}$) . ومن (3) نحصل على (5) $a = -\dfrac{b^2}{2c}$ ، $c \neq 0$.

($c = 0$ تؤدى إلى نفس التناقض السابق) . من (4) ، (5) نحصل على (6)

$a^2 = \dfrac{bc}{2}$ ، وبالتعويض من (6) فى (1) نحصل على : $a = \pm\dfrac{1}{\sqrt{3}}$ وهذا تناقض

كما سبق . وينتج المطلوب مباشرة .

<u>مثال ٤٨</u> : برهن على أن امتداد الحقل $\mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) \supset \mathbb{Q}$ بسيط

<u>البرهان</u> : سنبرهن على أن $\mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) = \mathbb{Q}(i + \sqrt{5})$.

"$\supset$" : واضح . سنبرهن الآن على الاحتواء الآخر "$\subset$" : كالآتى :

$$i + \sqrt{5} \in \mathbb{Q}(i + \sqrt{5}) \Rightarrow 4 + 2i\sqrt{5} = -1 + 2i\sqrt{5} + 5 = (i + \sqrt{5})^2 \in \mathbb{Q}(i + \sqrt{5})$$

$$\Rightarrow 14i + 2\sqrt{5} = (i + \sqrt{5})(4 + 2i\sqrt{5}) \in \mathbb{Q}(i + \sqrt{5})$$

$$\Rightarrow -12i = 2(i + \sqrt{5}) - 14i - 2\sqrt{5} \in \mathbb{Q}(i + \sqrt{5}) \Rightarrow i \in \mathbb{Q}(i + \sqrt{5})$$

$$\Rightarrow \sqrt{5} = i + \sqrt{5} - i \in \mathbb{Q}(i + \sqrt{5}) \Rightarrow i, -i, \sqrt{5}, -\sqrt{5} \in \mathbb{Q}(i + \sqrt{5})$$

<u>مثال ٤٩</u> : اوجد الحقول الجزئية من $\mathbb{C}$ المتولدة بـــ :

(١) $\{0, 1\}$ (٢) $\{0\}$

(٣) $\{0, 1, i\}$ (٤) $\{i, \sqrt{2}\}$

(٥) $\{\sqrt{2}, \sqrt{3}\}$ (٦) $\mathbb{R}$

(٧) $\mathbb{R} \cup \{i\}$

الحل : (١) $\mathbb{Q}$

(٢) لايوجد (الحقل يحتوى على عنصرين على الأقل ! فلا يمكن أن يكون الحقل الجزئى $\{0\}$)

(٣) $\{p+iq \mid p,q \in \mathbb{Q}\}$

(٤) $\{a+ib+\sqrt{2}c+i\sqrt{2}d \mid a,b,c,d \in \mathbb{Q}\}$

(٥) $\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\}$

(٦) $\mathbb{R}$

(٧) $\mathbb{C}$

مثال ٥٠ : صف الحقول الجزئية من $\mathbb{C}$ التى على الشكل :

(١) $\mathbb{Q}(\sqrt{2})$ (٢) $\mathbb{Q}(i)$

(٣) $\mathbb{Q}(\alpha)$ حيث α هو الجذر التكعيبى الحقيقى لـ 2

(٤) $\mathbb{Q}(\sqrt{5},\sqrt{7})$ (٥) $\mathbb{Q}(i,\sqrt{11})$

الحل :

(١) $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

(٢) $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\}$

(٣) $\mathbb{Q}(\alpha) = \{a+b\alpha+c\alpha^2 \mid a,b,c \in \mathbb{Q}\}$

(٤) $\mathbb{Q}(\sqrt{5},\sqrt{7}) = \{a+b\sqrt{5}+c\sqrt{7}+d\sqrt{35} \mid a,b,c,d \in \mathbb{Q}\}$

(٥) $\mathbb{Q}(i,\sqrt{11}) = \{a+bi+c\sqrt{11}+d\sqrt{11}i \mid a,b,c,d \in \mathbb{Q}\}$

مثال ٥١ : ليكن $K=\mathbb{Z}_2$. صف الحقول الجزئية من $K(t)$ التى على الشكل :

(١) $K(t^2)$ (٢) $K(t+1)$

(٣) $K(t^5)$ (٤) $K(t^2+1)$

الحل :

(١) عناصر الحقل الجزئى هى كل التعبيرات الخالية من القوى الفردية لـ t

(٢) $K(t)$

(٣) عناصر الحقل الجزئى هى كل التعبيرات التى قوى t فيها مضاعفات 5

(٤) تماما مثل (١)

مثال ٥٢ : عين أى امتدادات الحقول فى مثالى ٥٠ ، ٥١ يكون امتداداً جبرياً بسيطاً ، أو متسامياً بسيطاً .

الحل : الامتدادات فى مثال ٥١ كلها متسامية بسيطة . فى مثال ٥٠ الامتدادات الأربعة الأولى جبرية بسيطة. الامتداد الأخير (٥) جبرى لكنه ليس بسيطاً. لبيان أن الامتداد (٤) فى مثال ٥٠ بسيط ، نثبت أن

$$\mathbb{Q}(\sqrt{5},\sqrt{7}) = \mathbb{Q}(\sqrt{5}+\sqrt{7})$$

"$\supset$" : واضح . لبيان "$\subset$" :

$$(\sqrt{5}+\sqrt{7})^{-1} = \frac{1}{\sqrt{5}+\sqrt{7}} = \frac{\sqrt{7}-\sqrt{5}}{(\sqrt{7}-\sqrt{5})(\sqrt{7}+\sqrt{5})} = \frac{\sqrt{7}-\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5}+\sqrt{7})$$

$$\Rightarrow \sqrt{7}-\sqrt{5} \in \mathbb{Q}(\sqrt{5}+\sqrt{7}) \Rightarrow \sqrt{5},\sqrt{7} \in \mathbb{Q}(\sqrt{5}+\sqrt{7})$$

(انظر مثال ٣٩) .

مثال ٥٣ : حدد : أى التقارير الآتية صحيح وأيها خاطئ :

(١) كل حقل له امتداد غير تافه

(٢) كل حقل له امتداد جبرى غير تافه

(٣) كل امتداد بسيط يكون جبرياً

(٤) كل امتداد يكون بسيطاً

(٥) كل الامتداد الجبرية البسيطة تكون متشاكلة (أيزومورفية)

(٦) كل الامتدادات المتسامية البسيطة لحقل ما تكون متشاكلة

(٧) كل كثيرة حدود صغرى تكون مطبعة

(٨) كثيرات الحدود المطبعة تكون دائماً غير قابلة للتبسيط (للتحليل)

(٩) كل كثيرة حدود هى حاصل ضرب ثابت فى كثيرة حدود غير قابلة للتبسيط .

الحل : (١) ، (٦) ، (٧) صحيحة والباقى خاطئ

مثال ٥٤ : ليكن K امتداداً للحقل F . وليكن K_1 ، K_2 امتدادين للحقل F يحتويهما الحقل K . إذا كان $[E_1 : F]$ ، $[E_2 : F]$ عددين أوليين ، فبرهن على أن $E_1 = E_2$ أو $E_1 \cap E_2 = F$

البرهان : ليكن $E_1 \cap E_2 \neq F$. عندئذ فإنه من نظرية الدرجة يكون :

عدد أولى $[E_1 : F] = [E_1 : E_1 \cap E_2][E_1 \cap E_2 : F]$

ولأن $E_1 \cap E_2 \neq F$ فإن $[E_1 \cap E_2 : F] \neq 1$ ، ولأن $[E_1 : F]$ عدد أولى فينتج أن $[E_1 : E_1 \cap E_2] = 1$ ، أى أن $E_1 = E_1 \cap E_2$ ، وبالمثل نثبت أن $E_2 = E_1 \cap E_2$ وينتج المطلوب مباشرة .

مثال ٥٥ : ليكن $p(X) \in F[X]$ ، E امتداداً منتهياً للحقل F . إذا كانت $p(X)$ غير قابلة للتحليل (للتبسيط) على F (بعبارة مكافئة فى $F[X]$) ، وكان $(\deg(p(X)), [E : F]) = 1$ (أى ليس بينهما قواسم مشتركة غير الواحد) فبرهن على أن $p(X)$ غير قابلة للتحليل على E .

البرهان : ليكن a صفراً لـــ $p(X)$ فى امتداد ما لـــ F . لاحظ أولاً أن : $[E(a) : E] \leq [F(a) : F] = \deg(p(X))$. كذلك لاحظ أن :

$$[E(a) : F(a)][F(a) : F] = [E(a) : E][E : F]$$

وهذا يستلزم أن $\deg(p(X))$ يقسم $[E(a) : E]$ ، (لأن $(\deg(p(X)), [E : F]) = 1$) ، وبالتالى فإن

$$\deg(p(X)) = [E(a) : E]$$

وينتج المطلوب .

مثال ٥٦ : برهن على أن الجدولين الآتيين يعرفان حقلاً

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

.	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

اوجد حقله الأولى ومميزه . هل هذا الحقل يشاكل $\mathbb{Z}_4$ ؟ كم عدد الحقول - بدون حساب الأيزومورفيزمات (التشاكلات) - التى تتكون بالضبط من أربعة عناصر ؟

الحل : يترك للقارئ التحقق من أن الجدولين يعرفان حقلاً .

واضح أن الحقل الأولى هو $\mathbb{Z}_2$. ومميز الحقل - بالطبع - هو 2 . الحقل المعرف لا يشاكل $\mathbb{Z}_4$ لأن $\mathbb{Z}_4$ ليس حقلاً (بل هو حلقة إبدالية ذات عنصر الوحدة) . يوجد حقل واحد يتكون بالضبط من أربعة عناصر ، كما سنرى عندما ندرس الحقول المنتهية .

مثال ٥٧ : اوجد كثيرات الحدود الصغرى على الحقول "الصغيرة" للعناصر الآتية فى الامتدادات الآتية:

(أ) $i \in \mathbb{C} \supset \mathbb{Q}$

(ب) $i \in \mathbb{C} \supset \mathbb{R}$

(جـ) $\sqrt{2} \in \mathbb{R} \supset \mathbb{Q}$

(د) $(\sqrt{5}+1)/2 \in \mathbb{C} \supset \mathbb{Q}$

(هـ) $(i\sqrt{3}-1)/2 \in \mathbb{C} \supset \mathbb{Q}$

(و) $\alpha \in K \supset P$ حيث K الحقل فى مثال ٥٦ السابق مباشرة ، P حقله الأولى

(ز) $\alpha \in \mathbb{Z}_3(t)(\alpha) \supset \mathbb{Z}_3(t)$ حيث t غير محدد ، $\alpha^2 = t+1$

الحل :

(أ) لدينا $t = i$ ومن ثم فإن $t^2 + 1 = 0$ فنعرف كثيرة الحدود الصغرى ، هى $f := t^2 + 1$

(ب) تماماً مثل (أ)

(جـ) ضع $t = \sqrt{2}$ ومن ثم فإن $t^2 - 2 = 0$ ، فتكون كثيرة الحدود الصغرى هى: $f := t^2 - 2$

(د) ضع $t = \dfrac{\sqrt{5}+1}{2}$ وبالتالى فإن : $2t - 1 = \sqrt{5}$ ومن ثم فإن : $4t^2 - 4t + 1 = 5$ ،

أى أن $t^2 - t - 1 = 0$ فتكون كثيرة الحدود الصغرى هى : $f := t^2 - t - 1$

(هـ) ضع $t = \dfrac{i\sqrt{3}-1}{2}$ هذا يقتضى أن $2t + 1 = i\sqrt{3}$ ومن ثم فإن : $4t^2 + 4t + 1 = -3$

أى أن $t^2 + t + 1 = 0$ ، فتكون كثيرة الحدود الصغرى هى : $f := t^2 + t + 1$

(و) من جدول الضرب "." لدينا $\alpha^2 = \beta$ ، ومن جدول الجمع لدينا $\beta = \alpha + 1$ فواضح أن كثيرة الحدود الصغرى ستكون : $t^2 - t - \bar{1}$ أى هى $f := t^2 + t + \bar{1}$ (مميز الحقل=2).

(لاحظ أن هناك تماثلاً فى الجدول ، فكذلك $\beta^2 = \alpha$ ، $\beta = \alpha + 1$)

(ز) كثيرة الحدود الصغرى هى : $f := X^2 - t - 1$

(معتبرة ككثيرة حدود فى X) لأنها مطبعة : معامل X^2 هو الواحد ، وهى غير قابلة للتحليل فى $\mathbb{Z}_3(t)$ ، $f(\alpha) = t + 1 - t - 1 = 0$

مثال ٥٨ : حدد إذا ما كانت التقارير الآتية صائبة أم خاطئة :

(١) الامتدادات ذات الدرجة نفسها تكون متشاكلة

(٢) الامتدادات المتشاكلة يكون لها نفس الدرجة

(٣) كل امتداد متسام يكون غير منته

(٤) كل عنصر فى $\mathbb{C}$ يكون جبرياً على $\mathbb{R}$

(٥) كل امتداد لـــ $\mathbb{R}$ يكون منتهياً

(٦) كل امتداد جبرى لـــ $\mathbb{Q}$ يكون منتهياً

(٧) حقل الأعداد الجبرية هو أكبر حقل حقل جزئى فى $\mathbb{C}$ يكون جبرياً على $\mathbb{Q}$

(٨) كل فراغ خطى يكون متشاكلاً مع الفراغ الخطى المناظر لامتداد حقل ما

(٩) كل امتداد لحقل منته يكون منتهياً

الحل : (٢) ، (٣) ، (٤) ، (٧) ، (٨) صحيحة . الباقى خاطئ

مثال ٥٩ : كثيرة الحدود $X^3 - 1 \in \mathbb{Q}[X]$ تتشقق على $\mathbb{C}$ لأننا يمكننا أن نكتب :

$$X^3 - 1 = (X - 1)(X - \omega)(X - \omega^2)$$

حيث $1, \omega, \omega^2$ الجذور التكعيبية للواحد ، أى أن $\omega = e^{\frac{2\pi i}{3}}$ لكننا فى مثال ١٩ أوجدنا **حقل التشقيق** لكثيرة الحدود وهو $\mathbb{Q}\sqrt{-3}$.

مثال ٦٠ : اوجد حقل التشقيق لكثيرة الحدود $X^4 - 4X^2 - 5 \in \mathbb{Q}[X]$

الحل :

$$\begin{aligned} X^4 - 4X^2 - 5 &= (X^2 - 5)(X^2 + 1) \\ &= (X - \sqrt{5})(X + \sqrt{5})(X - i)(X + i) \end{aligned}$$

ومن ثم فإن حقل تشقيق كثيرة الحدود المعطاة هو : $\mathbb{Q}(\sqrt{5}, i)$

مثال ٦١ : اوجد حقل تشقيق كثيرة الحدود $f := t^5 - 3t^3 + t^2 - 3 \in \mathbb{Q}[t]$

الحل :

$$\begin{aligned} f := t^5 - 3t^3 + t^2 - 3 &= (t^2 - 3)(t^3 + 1) \\ &= (t + \sqrt{3})(t - \sqrt{3})(t + 1)(t^2 - t + 1) \\ &= (t + \sqrt{3})(t - \sqrt{3})(t + 1)(t - \frac{1 + i\sqrt{3}}{2})(t - \frac{1 - i\sqrt{3}}{2}) \end{aligned}$$

واضح أن حقل التشقيق هو $\mathbb{Q}(\sqrt{3}, -\sqrt{3}, \frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2})$

وهو نفس الحقل $\mathbb{Q}(\sqrt{3}, \frac{1+i\sqrt{3}}{2})$ (لماذا ؟)

وهو نفس الحقل $\mathbb{Q}(\sqrt{3}, i)$ (لماذا ؟)

لكن ليس هو الحقل $\mathbb{Q}(\sqrt{3}i)$. واضح أن $\mathbb{Q}(\sqrt{3}i)\subsetneq\mathbb{Q}(\sqrt{3},i)$

مثال ٦٢ : اوجد حقل تشقيق $f := (X^2-2X-2)(X^2+1)\in\mathbb{Q}[X]$

الحل : أصفار f فى $\mathbb{C}$ هى : $\pm i, 1\pm\sqrt{3}$. وبهذا يكون

حقل تشقيق f هو : $\mathbb{Q}(i,-i,1+\sqrt{3},1-\sqrt{3})$

وهو نفس الحقل $\mathbb{Q}(i,\sqrt{3})$ (لماذا ؟)

أى هو نفس حقل كثيرة الحدود فى مثال ٦١ على الرغم من أن كثيرتى الحدود مختلفتان .

مثال ٦٣ : مدخل آخر مختلف قليلاً عن المدخل فى مثال ٨ السابق . كما ذكرنا فى الملحوظة عقب مثال٨ فإننا لانستخدم $\mathbb{C}$. ولهذا فإننا يجب أن نعتمد على التكوين الأساسى لحقل تشقيق كثيرة الحدود $f := X^2+X+\bar{1}$ على $\mathbb{Z}_2$.

الحقل $\mathbb{Z}_2$ يتكون من عنصرين $\bar{0}$ ، $\bar{1}$. نلاحظ أن f غير قابلة للتبسيط (للتحليل) على $\mathbb{Z}_2$ ، ولهذا سنضم (سنلحق) عنصراً η بحيث يكون η لها كثيرة الحدود الصغرى f على $\mathbb{Z}_2$. عندئذ فإن : $\eta^2+\eta+\bar{1}=\bar{0}$ ، أى أن $\eta^2=\eta+\bar{1}$ (مميز الحقل = 2). نحن ندعى أن الأربعة عناصر الآتية تكون حقلاً

$$\bar{0},\bar{1},\eta,\bar{1}+\eta$$

وللبرهنة على ذلك سننشئ جدولى الجمع والضرب

$+$	0	$\bar{1}$	η	$\bar{1}+\eta$
0	0	$\bar{1}$	η	$\bar{1}+\eta$
$\bar{1}$	$\bar{1}$	0	$\bar{1}+\eta$	η
η	η	$\bar{1}+\eta$	0	$\bar{1}$
$\bar{1}+\eta$	$\bar{1}+\eta$	η	$\bar{1}$	0

$\cdot$	0	$\bar{1}$	η	$\bar{1}+\eta$
0	0	0	0	0
$\bar{1}$	0	$\bar{1}$	η	$\bar{1}+\eta$
η	0	η	$\bar{1}+\eta$	$\bar{1}$
$\bar{1}+\eta$	0	$\bar{1}+\eta$	$\bar{1}$	η

مثال للحساب :

$$\eta(\bar{1}+\eta)=\eta+\eta^2=\eta+\bar{1}+\eta=\bar{2}\eta+\bar{1}=\bar{0}+\bar{1}=\bar{1}$$

أى أن $\mathbb{Z}_2(\eta)$ حقل ذو أربعة عناصر . والآن f تتشقق على $\mathbb{Z}_2(\eta)$. ولبيان ذلك نجرى القسمة المطولة

$$\begin{array}{r|l} & X+\bar{1}+\eta \\ X-\eta & X^2+X+\bar{1} \\ & X^2-\eta X \\ \hline & (\bar{1}+\eta)X+\bar{1} \\ & (\bar{1}+\eta)X-\eta-\eta^2 \\ \hline & \bar{1}+\eta+\eta^2=\bar{0} \end{array}$$

أى أن $X^2+X+\bar{1}=(X-\eta)(X+\bar{1}+\eta)$

$$=(X-\eta)(X-\bar{1}-\eta)$$

(المميز = 2)

f تتشقق على $\mathbb{Z}_2(\eta)$ ، لكنها لا تتشقق على حقل أصغر منه .

أى أن $\mathbb{Z}_2(\eta)$ هو حقل تشقيق f .

<u>مثال ٦٤</u> : حدد : أى التقريرين الآتيين صحيح ، وأيهما خاطئ :

(١) كل كثيرة حدود تتشقق على حقل ما

(٢) حقول التشقيق وحيدة ، بدون حساب الأيزومورفيزمات

<u>الحل</u> : التقريران صحيحان

<u>مثال ٦٥</u> : حدد : أى التقارير الآتية صائب وأيها خاطئ :

(١) إذا كان $\alpha,\beta\in E$ ، حيث $E\subset\overline{F}$ حقل تشقيق على F فإنه يوجد أوتومورفيزم لـــ E (أى أيزومورفيزم من E إلى E) يترك F ثابتاً ، ويرسم α على

β إذا كانت وفقط إذا كانت كثيرة الحدود الصغرى من α على F هى نفس كثيرة الحدود الصغرى من β على F .

(٢) $\mathbb{R}$ حقل تشقيق على $\mathbb{Q}$

(يقال إن E حقل تشقيق على الحقل F إذا كان E حقل تشقيق لبعض كثيرات الحدود فى $F[X]$)

(٣) $\mathbb{R}$ حقل تشقيق على $\mathbb{R}$

(٤) $\mathbb{C}$ حقل تشقيق على $\mathbb{R}$

(٥) $\mathbb{Q}(i)$ حقل تشقيق على $\mathbb{Q}$

(٦) $\mathbb{Q}(\pi)$ حقل تشقيق على $\mathbb{Q}(\pi^2)$

(٧) لكل حقل تشقيق E على F ، حيث $E \subset \overline{F}$ كل راسم أيزومورفى (isomorphic mapping) لـــ E إلى $\overline{F}$ يكون أوتومورفيزماً لـــ E

(٨) لكل حقل تشقيق E على F ، حيث $E \subset \overline{F}$ (انظر مثال ٤٢) ، كل أيزومورفيزم يرسم E فى $\overline{F}$ هو أوتومورفيزم لـــ E

(٩) لكل حقل تشقيق E على F ، حيث $E \subset \overline{F}$ ، كل أيزومورفيزم يرسم E فى $\overline{F}$ ، تاركاً F ثابتاً ، هو أوتومورفيزم لـــ E

(١٠) كل إغلاق جبرى $\overline{F}$ لـــ F هو حقل تشقيق على F

<u>**الحل**</u> : (٢) ، (٧) ، (٨) خاطئة . باقى التقارير صحيحة .

<u>**مثال ٦٦**</u> : اوجد حقل تشقيق كثيرة الحدود $X^3 - 2 \in \mathbb{Q}[X]$ على $\mathbb{Q}$. ما درجة امتداد حقل التشقيق على $\mathbb{Q}$ ؟

<u>**الحل**</u> :

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$$

$$X^2 + \sqrt[3]{2}X + \sqrt[3]{4} = 0 \Rightarrow X = \frac{-\sqrt[3]{2} \pm \sqrt{\sqrt[3]{4} - 4\sqrt[3]{4}}}{2}$$

$$= \frac{\sqrt[3]{2}[-1 \pm \sqrt{-3}]}{2} = \frac{\sqrt[3]{2}[-1 \pm \sqrt{3}i]}{2}$$

وبالتالى فإن حقل التشقيق المطلوب هو : $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ (لماذا ؟)

(لاحظ أن $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$)

والآن : $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(i\sqrt{3})] = 3$

لأن $\deg(X^3 - 2) = 3$ ، حيث $X^3 - 2$ هى كثيرة الحدود الصغرى من $\sqrt[3]{2}$ على $\mathbb{Q}$

كذلك فإن : $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$

لأنه بوضع $X = i\sqrt{3}$ ينتج أن : $X^2 + 3 = 0$

وتكون $X^2 + 3$ هى كثيرة الحدود الصغرى من $i\sqrt{3}$ على $\mathbb{Q}$ ودرجتها 2

وبالتالى فإنه من نظرية الدرجة يكون

$$[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(i\sqrt{3})][\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}]$$
$$= 3 . 2 = 6$$

<u>مثال ٦٧</u> : اوجد حقل تشقيق $\{X^2 - 2, X^2 - 3\}$ على $\mathbb{Q}$

<u>الحل</u> : حقل التشقيق المطلوب هو $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

<u>مثال ٦٨</u> : اوجد حقل تشقيق $f := (X^2 - 2)(X^3 - 2) \in \mathbb{Q}[X]$ على $\mathbb{Q}$.

واوجد درجته : (أى درجة الامتداد لحقل التشقيق على الحقل $\mathbb{Q}$)

<u>الحل</u> : $(X^2 - 2)(X^3 - 2) = 0 \Rightarrow X = \pm\sqrt{2}, \sqrt[3]{2}, \alpha, \beta$

حيث α, β جذرا المعادلة $X^2 + \sqrt[3]{2}X + \sqrt[3]{4} = 0$

أى هما $\dfrac{\sqrt[3]{2}[-1 \pm \sqrt{3}i]}{2}$

(انظر مثال ٦٦ السابق)

وبهذا يكون حقل التشقيق هو $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt{3}i)$

لإيجاد الدرجة :

$$\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt{3}i) = (\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i))(\sqrt{2})$$

$$[(\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i))(\sqrt{2}) : \mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)] = 2$$

$$[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$$ (من مثال ٦٦)

ومن ثم فإن :

$$[\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt{3}i) : \mathbb{Q}] = 6.2 = 12$$

مثال ٦٩ : ليكن α صفرا لـ $X^3+X^2+\bar{1}$ على $\mathbb{Z}_2$. برهن على أن $X^3+X^2+\bar{1}$ تتشقق على $\mathbb{Z}_2(\alpha)$. اوجد صفرين آخرين بالإضافة إلى α لـ $X^3+X^2+\bar{1}$

الحل : إذا كانت α صفرا لـ $X^3+X^2+\bar{1}$ على $\mathbb{Z}_2$ فإن :

$\alpha^3+\alpha^2+\bar{1}=\bar{0}$. والآن $X-\alpha$ عامل من عوامل $X^3+X^2+\bar{1}$ فنستخدم القسمة المطولة كالآتى :

$$\begin{array}{r|l}
 & X^2+(\alpha+\bar{1})X+\alpha^2+\alpha \\
X-\alpha & X^3+X^2+\bar{1} \\
 & X^3-\alpha X^2 \\
\hline
 & (\alpha+\bar{1})X^2+\bar{1} \\
 & (\alpha+1)X^2-\alpha^2X-\alpha X \\
\hline
 & (\alpha^2+\alpha)X+\bar{1} \\
 & (\alpha^2+\alpha)X-\alpha^3-\alpha^2 \\
\hline
 & \alpha^3+\alpha^2+\bar{1}=0
\end{array}$$

أى أن

$$X^3+X^2+\bar{1}=(X-\alpha)[X^2+(\alpha+\bar{1})X+\alpha^2+\alpha]$$

واضح أن α^2 صفر آخر لكثيرة الحدود $X^3+X^2+\bar{1}$ ، لأنه صفر لكثيرة الحدود $X^2+(\alpha+\bar{1})X+\alpha^2+\alpha$ ، كما يتضح مما يأتى بالتعويض عن X بـ α^2 :

$$\alpha^4+\alpha^3+\alpha^2+\alpha^2+\alpha=\alpha^4+\alpha^3+\bar{2}\alpha^2+\alpha=\alpha^4+\alpha^3+\alpha=\alpha(\alpha^3+\alpha^2+\bar{1})$$

$$=\alpha.\bar{0}=\bar{0}$$

كذلك فإن $\bar{1}+\alpha+\alpha^2$ صفر لكثيرة الحدود $X^3+X^2+\bar{1}$ ، لأنه بالتعويض عن X فى $X^2+(\alpha+\bar{1})X+\alpha^2+\alpha$ بـ $\bar{1}+\alpha+\alpha^2$ نحصل على :

$$(\alpha^2+\alpha+\bar{1})^2+(\alpha+\bar{1})(\alpha^2+\alpha+\bar{1})+\alpha^2+\alpha$$

$$=\alpha^4+\alpha^2+\bar{1}+\bar{2}\alpha^3+\bar{2}\alpha^2+\bar{2}\alpha+\alpha^3+\alpha^2+\alpha+\alpha^2+\alpha+\bar{1}+\alpha^2+\alpha$$

$$=\alpha^4+\bar{3}\alpha^3+\bar{6}\alpha^2+\bar{5}\alpha+\bar{2}=\alpha^4+\alpha^3+\alpha=\alpha(\alpha^3+\alpha^2+\bar{1})=\alpha.\bar{0}=\bar{0}$$

(الحساب فى $\mathbb{Z}_2$) . ومن حيث إن كثيرة الحدود من الدرجة الثالثة ، ولدينا أصفار ثلاثة ، فيكون $\mathbb{Z}_2(\alpha)$ حقل التشقيق لها .

<u>**ملحوظة**</u> : لاحظ أن $\mathbb{Z}_2(\alpha)$ يتكون من ثمانية عناصر هى :

$b_0+b_1\alpha+b_2\alpha^2,\ \ b_0,b_1,b_2\in\mathbb{Z}_2$ راجع مثال ٧ .

تمارين عامة (١)

(١) لكل من الأعداد $\alpha\in\mathbb{C}$ الآتية ، برهن على أن α جبرى على $\mathbb{Q}$ بإيجاد $f\in\mathbb{Q}[X]$ بحيث يكون $f(\alpha)=0$.

(أ) $1+\sqrt{2}$ (ب) $\sqrt{2}+\sqrt{3}$

(جـ) $\sqrt{1+\sqrt[3]{2}}$ (د) $1+i$

(هـ) $\sqrt{\sqrt[3]{2}-i}$

(٢) (أ) برهن على أن كثيرة الحدود X^2+1 غير قابلة للتحليل (للتبسيط) فى $\mathbb{Z}_3[X]$

(ب) ليكن α صفراً لكثيرة الحدود X^2+1 فى امتداد للحقل $\mathbb{Z}_3$. اكتب جدولى الجمع والضرب للعناصر التسعة فى $\mathbb{Z}_3(\alpha)$ مكتوبة فى الترتيب :

$\bar{0}$ ، $\bar{1}$ ، $\bar{2}$ ، α ، $\bar{2}\alpha$ ، $\bar{1}+\alpha$ ، $\bar{1}+\bar{2}\alpha$ ، $\bar{2}+\alpha$ ، $\bar{2}+\bar{2}\alpha$.

(٣) برهن على أنه يوجد حقل مكون من 49 عنصرا

(٤) برهن على أنه يوجد حقل مكون من 125 عنصراً

(٥) اوجد درجة كل من امتدادات الحقول الآتية :

(أ) $\mathbb{Q}(7)\supset\mathbb{Q}$ (ب) $\mathbb{Q}(\sqrt{2},\sqrt{5})\supset\mathbb{Q}$

(جـ) $\mathbb{Q}(\sqrt{2},\sqrt[3]{5})\supset\mathbb{Q}$ (د) $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24})\supset\mathbb{Q}$

(٦) ما درجة امتداد الحقول التى يمكننا أن نحصل عليها بإلحاق بالتتابع جذر تربيعى لعنصر بحقل F ، وهذا العنصر ليس مربعاً فى F ، ثم إلحاق جذر تربيعى لعنصر وهذا العنصر ليس مربعاً فى الحقل الجديد ، وهكذا ... ؟

(٧) عين عناصر $\mathbb{Q}(\sqrt[3]{7})$

(٨) اوجد حقل التشقيق لكثيرة الحدود

$$X^4+X^2+1=(X^2+X+1)(X^2-X+1)$$

على $\mathbb{Q}$. عبر عن الإجابة فى شكل $\mathbb{Q}(a)$

(٩) طبق ما أديناه فى مثال ٩ على الآتى :

لتكن $f:=X^5+2X^2+2X+2\in\mathbb{Z}_3[X]$. (لاحظ أن $f=(X^2+1)(X^3+2X+2)$)

(١٠) لتكن α جبرية على $\mathbb{Q}$. برهن على أن $\sqrt{\alpha}$ جبرى على $\mathbb{Q}$.

(١١) اوجد درجة الامتداد $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ على $\mathbb{Q}(\sqrt{3},\sqrt{5})$ وأساسا له

(١٢) اوجد درجة الامتداد $\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2})\supset\mathbb{Q}$ وأساسا له

(١٣) اوجد كثيرة الحدود الصغرى لـ $\sqrt[3]{2}+\sqrt[3]{4}$ على $\mathbb{Q}$.

(١٤) اوجد حقل تشقيق كثيرة الحدود $X^4-X^2-\bar{2}$ على $\mathbb{Z}_3$

(١٥) برهن على أن $\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2},...)$ هو امتداد جبرى لـ $\mathbb{Q}$ لكنه ليس منتهيا

(١٦) إذا كان E إغلاقا جبريا لـ F ، فبرهن على أن كل كثيرة حدود غير ثابتة فى $F[X]$ تتشقق على E

(١٧) ليكن E امتداداً جبرياً لـ F . إذا كانت كل كثيرة حدود فى $F[X]$ تتشقق على E ، فبرهن على أن E مغلق جبرياً .

(١٨) ليكن F حقلاً وكل كثيرة حدود غير قابلة للتحليل فى $F[X]$ خطية . برهن على أن F مغلق جبرياً

(١٩) ليكن E امتداداً للحقل F ودرجة الامتداد عدد أولى. برهن على أنه لكل $a\in E$

$F(a)=E$ أو $F(a)=F$

(٢٠) اوجد كثيرتى الحدود الصغريين من $\sqrt{2}$ على $\mathbb{R}$ ، على $\mathbb{Q}$

(٢١) برهن على أن $\mathbb{R}$ ليست امتداداً بسيطاً لـ $\mathbb{Q}$ كالآتى :

(١) $\mathbb{Q}$ قابلة للعد (countable)

(٢) أى امتداد بسيط لحقل قابل للعد يكون قابلاً للعد

(٣) $\mathbb{R}$ ليست قابلة للعد

(٢٢) ليكن K امتداداً للحقل F ، وليكن $a\in K$. برهن على أن : $[F(a):F(a^3)]=1$ أو $[F(a):F(a^3)]=3$

(٢٣) اضرب مثالاً لامتداد جبرى يحتوى على عناصر من كل درجة على $\mathbb{Q}$

(٢٤) لتكن $m(t)$ كثيرة حدود غير قابلة للتحليل على K ، α لها كثيرة الحدود الصغرى $m(t)$ على K. هل تتحلل $m(t)$ بالضرورة على $K(\alpha)$ إلى كثيرات حدود خطية (أى لها الدرجة 1) ؟

(٢٥) لأى من القيم الآتية لـ $m(t)$ توجد امتدادات $K(\alpha)$ لـ K بحيث تكون α لها كثيرة الحدود الصغرى $m(t)$ ؟

(أ) $m(t)=t^2-4, K=\mathbb{R}$

(ب) $m(t)=t^2+1, K=\mathbb{Z}_3$

(جـ) $m(t)=t^2+1, K=\mathbb{Z}_5$

(د) $m(t)=t^7-3t^6+4t^3-t-1, K=\mathbb{R}$

(٢٦) اوجد درجات الامتدادات الآتية :

(١) $\mathbb{C}\supset\mathbb{Q}$ (٢) $\mathbb{Z}_5(t)\supset\mathbb{Z}_5$

(٣) $\mathbb{R}(\sqrt{5})\supset\mathbb{R}$ (٤) $\mathbb{Q}(\alpha)\supset\mathbb{Q}$ حيث α هو الجذر التكعيبى الحقيقى لـ 2

(٥) $\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{11})\supset\mathbb{Q}$ (٦) $\mathbb{Q}(\sqrt{7})\supset\mathbb{Q}$

(٧) $\mathbb{Q}(\alpha)\supset\mathbb{Q}$ حيث $\alpha^7=3$

(الإجابة : (١) ∞ (٢) ∞ (٣) 1 (٤) 3

(٥) 8 (٦) 2 (٧) 7)

(٢٧) برهن على أن أى عنصر فى $\mathbb{Q}(\sqrt{5},\sqrt{7})$ يمكن أن يعبر عنه بطريقة وحيدة كالآتى:

$$p+q\sqrt{5}+r\sqrt{7}+s\sqrt{35}$$

حيث p ، q ، r ، s عناصر فى $\mathbb{Q}$.

(٢٨) إذا كانت $K=K_0\subset K_1\subset\ldots\subset K_r=L$ حقولا ، فبرهن على أن :

$$[L:K]=[K_r:K_{r-1}]\ldots[K_2:K_1][K_1:K_0]$$

(٢٩) اعتبر امتداد الحقل $\mathbb{Q}(\sqrt{1+\sqrt{3}})\supset\mathbb{Q}$. عين درجة امتداد الحقل واوجد أساساً له .

(٣٠) ليكن $L \supset k$ امتداد حقل . برهن على أن الضرب بعنصر ثابت من L هو تحويل خطى (linear transformation) من L إلى L باعتبار L فراغا خطياً على K . متى يكون هذا التحويل الخطى لـــ L غير استثنائى ؟

(٣١) برهن على أن كثيرتى الحدود $X^2-3, X^2-2X-2 \in \mathbb{Q}[X]$ لهما نفس حقل التشقيق

(٣٢) اوجد حقول تشقيق على $\mathbb{Q}$ (تكون حقولاً جزئية من $\mathbb{C}$) لكثيرات الحدود الآتية :

$$t^6-8 \quad ، \quad t^4+5t^2+6 \quad ، \quad t^3-27$$

(٣٣) اوجد درجات الحقول كامتدادات لـــ $\mathbb{Q}$ فى مثال ٣٢ السابق مباشرة

(٣٤) أنشئ حقل تشقيق لكثيرة الحدود X^3+2X+1 على $\mathbb{Z}_3$

(٣٥) أنشئ حقل تشقيق لكثيرة الحدود X^3+X^2+X+2 على $\mathbb{Z}_3$. هل هو يشاكل ذلك المنشأ فى تمرين (٣٤) السابق مباشرة ؟

(٣٦) اسرد كل كثيرات الحدود المطبعة من الدرجة الثانية على $\mathbb{Z}_5$. أيها يكون غير قابل للتحليل (للتبسيط) ؟ أنشئ حقول تشقيق لبعض هذه غير القابلة للتحليل . هل هذه الحقول متشاكلة ؟ كم عدد عناصر هذه الحقول ؟

(٣٧) إذا كانت f كثيرة حدود من الدرجة n على K ، وكان L حقل تشقيق لـــ f على K ، فبرهن على أن $[L:K]$ يقسم $n!$

(٣٨) اوجد حقول التشقيق ودرجتها على $\mathbb{Q}$ لكثيرات الحدود الآتية فى $\mathbb{Q}[X]$:

(أ) X^2+3 (ب) X^4-1

(جـ) $(X^2-2)(X^2-3)$ (د) X^3-3

(٣٩) لتكن $f \in F[X]$. إذا كان $\deg(f)=2$ ، a صفراً لـــ f فى امتداد ما لـــ F . برهن على أن $F(a)$ حقل تشقيق لـــ f على F .

(٤٠) لتكن f كثيرة حدود فى $F[X]$ ، درجتها n . ليكن $E \subset \overline{F}$ هو حقل تشقيق f على F فى $\overline{F}$. ما حدود $[E:F]$ ؟

3 Field Theory نظرية الحقول

القسم



Golois Theory نظرية جالوا

٢-١ زمر جالوا Galois groups

٢-١-١ ملحوظة :

لكل حقل K:من الواضح أن مجموعة أوتومورفيزمات K مع تركيبها تكون زمرة (التركيب هو عملية الزمرة) ، يشار إليها بالرمز $Aut(K)$ وتسمى زمرة **أوتومورفيزمات K** (Automorphisms group of K)

٢-١-٢ تعريف :

(أ) ليكن $K \supset k$ امتداد حقل . المجموعة الآتية

$$Aut(K;k) := \{\varphi \in Aut(K) \mid \varphi(a) = a \quad \forall a \in k\}$$

تكون زمرة جزئية من $Aut(K)$ (البرهان مباشر تماماً !) وتسمى هذه الزمرة الجزئية **زمرة الأوتومورفيزمات النسبية لـــ** $K \supset k$ (The relative automorphisms of group) $K \supset k$(أو **زمرة جالوا لـــ** $K \supset k$ (Galois group of $K \supset k$) ، ويشار إليها أحيانا بالرمز $G(K/k)$

(ب) إذا كان k حقلاً ، f كثيرة حدود ليست ثابتة فى $k[X]$ ، $K \supset k$ حقل التشقيق لــ f ، يسمى $Gal(f;k) := Aut(K;k)$ **زمرة جالوا لــ f على k** (Galois group of f over k)

٢-١-٣ ملحوظة :

إذا كان P هو الحقل الأولى لحقل K ، فإن $Aut(K;P) = Aut\ K$

البرهان : "$\subset$" : واضح . نبرهن على أن $Aut(K) \subset Aut(K;P)$ ، أى نبرهن على أن $\forall x \in P \quad \forall \varphi \in Aut(K) : \varphi(x) = x$

ليكن 1 هو عنصر الوحدة فى K ، وبهذا يكون $\varphi(1) = 1$ لكل $\varphi \in Aut(K)$ ، وبالتالى يكون $\varphi(n.1) = \varphi(1 + ... + 1) = n\varphi(1) = n.1$ لكل $n \in \mathbb{N} \setminus \{0\}$ ،

ومن ثم فإن $\varphi(n.1)=n.1$ لكل $n\in\mathbb{Z}$. والآن لكل $x\in P$ يوجد $m,n\in\mathbb{Z}$

بحيث $n.1\neq 0$ ، $x=\dfrac{m.1}{n.1}$ (انظر (١-١-٩)) . ومن ثم فإن :

$$\forall\varphi\in Aut(K):\varphi(x)=\varphi(\frac{m.1}{n.1})=\frac{\varphi(m.1)}{\varphi(n.1)}=\frac{m.1}{n.1}=x$$

٢-١-٤ <u>ملحوظة</u> :

(١) ليكن $K\supset k$ امتداد حقل ، $\varphi\in Aut(K;k)$ ، $f\in k[X]$. إذا كان $a\in k$ صفراً لــ f ، فإن $\varphi(a)$ أيضاً صفر لــ f

(٢) ليكن k حقلاً ، $f\in k[X]$ ليست ثابتة ، $K\supset k$ حقل التشقيق لــ f ، N مجموعة أصفار f المختلفة فى K ، $n:=Ord(N)$ (n هى رتبة N) . فإن :

(أ) الراسم

$$Gal(f;k)\to\gamma_n$$
$$\varphi\mapsto\varphi|N$$

مونومورفيزم .

باختصار : زمرة جالوا لــ f هى زمرة جزئية من γ_n ، حيث n عدد الأصفار المختلفة لــ f فى حقل تشقيقها

(ب) إذا كانت f غير قابلة للتحليل (للتبسيط) ، فإن الراسم :

$$Gal(f;k)\times N\to N$$
$$(\varphi,a)\mapsto\varphi(a)$$

يكون عملية من $Gal(f;k)$ على N ، وهى عملية انتقالية

<u>البرهان</u> : (١) لأن $\varphi|k=1_k$ ينتج أن : $\forall a\in k: f(\varphi(a))=f(a)=\varphi(f(a))=\varphi(0)=0$

أى أن $\varphi(a)$ صفر لــ f

(٢) (راجع تعريف عملية G على X فى البند (٥-١-١) من نظريات سيلو . يقال للعملية τ من G على X إنها <u>انتقالية</u> (transitive) إذا كان لكل $(x,y)\in X\times X$ يوجد على الأقل $a\in G$ بحيث يكون $y=a(x)=:\tau(a,x)$)

والآن الراسم فى (أ) واضح أنه هومومورفيزم . وهو أيضاً راسم واحد لواحد لأن $k(N)=K$ ، ومن $\varphi|N=1_N$ ينتج أنه لجميع $\varphi(x)=x : x\in K$ ، أى أن $\varphi=1_K$. أى أن نواة الراسم تتكون من العنصر الصفرى فى $Gal(f;k)$ ، أى أن الراسم واحد لواحد (أحادى)

واضح أن الراسم فى (ب) عملية لأن :

$$\forall a,b\in N : \exists\varphi\in Gal(f;k) : \varphi(a)=b$$

$$\forall a\in\mathbb{N} \quad : 1_{Gal(f;k)}(a) := 1_{Aut(K;k)}(a)=a$$

وهى عملية انتقالية وينتج ذلك مباشرة من (١-٨-٧) بوضع $k'=k$ ، $\varphi=1_k$

<u>٢-١-٥ مثال</u> :

المطلوب البرهنة على أن زمرة جالوا لكثيرة الحدود $f:=(X^2-2)(X^2-3)\in\mathbb{Q}[X]$ على $\mathbb{Q}$ هى زمرة كلاين الرباعية . (انظر (١-٤-٤) ، مثال ٤٤ من أمثلة متنوعة فى الباب الأول من نظرية الزمر)

<u>البرهان</u> : واضح أن $\mathbb{Q}(\sqrt{2},\sqrt{3})\supset\mathbb{Q}$ هو حقل التشقيق لــ f . من (٢-١-٢) ، (٢-١-٣) يكون المطلوب هو تعيين زمرة الأوتومورفيزمات لــ $K:=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

لكل من هذه الأوتومورفيزمات يتحقق :

$$2=\varphi(2)=\varphi(\sqrt{2})^2=(\varphi(\sqrt{2}))^2\Rightarrow\varphi(\sqrt{2})\in\{\sqrt{2},-\sqrt{2}\}$$

وبالمثل $\varphi(\sqrt{3})\in\{\sqrt{3},-\sqrt{3}\}$. أى أنه يوجد على الأكثر أربعة أوتومورفيزمات لــK .

كثيرة الحدود X^2-3 غير قابلة للتبسيط (للتحليل) فى $\mathbb{Q}(\sqrt{2})[X]$ ، لأنها ليس لها أصفار فى $\mathbb{Q}(\sqrt{2})$. ولأن $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})=(\mathbb{Q}(\sqrt{2}))(-\sqrt{3})$ فإنه يوجد أوتومورفيزم φ_1 لــ K بحيث يكون لجميع $x\in\mathbb{Q}(\sqrt{2}) : \varphi_1(x)=x$ ، $\varphi_1(\sqrt{3})=-\sqrt{3}$ (انظر (١-٨-٣)). وبالمثل يوجد أوتومورفيزم φ_2 لــ K بحيث يكون $\varphi_2(\sqrt{3})=\sqrt{3}$ ،

$K:=\mathbb{Q}(\sqrt{2},\sqrt{3})$ أساس للفراغ الخطى $B:=\{1,\sqrt{2},\sqrt{3},\sqrt{2}\sqrt{3}\}$ ولأن . $\varphi_2(\sqrt{2})=-\sqrt{2}$

على $\mathbb{Q}$ ، ولكل $b\in B$: $\varphi_1^2(b)=\varphi_2^2(b)=b$ فإنه ينتج أن $\varphi_1^2=\varphi_2^2=1_K$. ومن

ثم فإنه ينتج أن $Aut(K)\neq\{1_K,\varphi_1,\varphi_2\}$ ، وإلا كان $Aut(K)$ زمرة دائرية وبالتالى

يجب أن تحتوى على عنصر رتبته 3 . ومن ثم فإنه يجب أن يوجد بالضبط أوتومورفيزم

رابع ، ومما سبق فهو يحقق : $\varphi(\sqrt{2})=-\sqrt{2}$ ، $\varphi(\sqrt{3})=-\sqrt{3}$ ، وبالتالى يحقق

كذلك $\varphi_3^2=1_K$

وبهذا يكون $Aut(K)=\{1_K,\varphi_1,\varphi_2,\varphi_3\}$

حيث $\varphi_1^2=\varphi_2^2=\varphi_3^2=1_K$ ، أى أن $Aut(K)$ هو زمرة كلاين الرباعية .

٢-٢ نظرية جالوا الأساسية

The Fundamental Theorem of Galois Theory

٢-٢-١ تعريف :

ليكن K حقلاً ، G زمرة جزئية من $Aut(K)$. نعرف $Fix\ (K;G)$ ويسمى **الحقل الثابت بـ G فى K** كالآتى :

$$Fix\,(K;G):=\{a\in K\mid \varphi(a)=a\quad \forall\varphi\in G\}$$

$Fix\,(K;G)$ حقل جزئى من K لأن :

$\forall a,b\in Fix\,(K;G), b\neq 0:$

$a,b\in K; b\neq 0:\varphi(a)=a,\varphi(b)=b\Rightarrow$

$[\varphi(a-b)=\varphi(a)-\varphi(b)=a-b\Rightarrow a-b\in Fix\,(K;G),$

$\varphi(ab^{-1})=\varphi(a)\varphi(b^{-1})=\varphi(a)\varphi(b)^{-1}=ab^{-1}\Rightarrow ab^{-1}Fix\,(K;G)];$

$\varphi(1)=1$ (1 عنصر الوحدة فى K)

أى أن $Fix\,(K;G)\neq\phi$

٢-٢-٢ تعريف :

ليكن $K\supset k$ امتداد حقل . يسمى هذا الامتداد **امتداد جالوا** (Galois extension) إذا وجدت G زمرة جزئية **منتهية** من $Aut(K)$ بحيث يكون $k=Fix\,(K;G)$

٢-٢-٣ مثال : امتداد الحقل $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ ليس امتداد جالوا .

سنبرهن على ذلك بالبرهنة على أن $Aut(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$ وبهذا يكون :

$$\begin{aligned} Fix(\mathbb{Q}(\sqrt[3]{2});\{1\}) &= \{a \in \mathbb{Q}(\sqrt[3]{2}) : 1(a) = a\} \\ &= \{a \in \mathbb{Q}(\sqrt[3]{2})\} = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q} \end{aligned}$$

والآن نبرهن على أن $Aut(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$ كالآتى :

من (٢-١-٣) $Aut(\mathbb{Q}(\sqrt[3]{2});\mathbb{Q}) = Aut(\mathbb{Q}(\sqrt[3]{2}))$ ($\mathbb{Q}$ هو الحقل الأولى فى $\mathbb{Q}(\sqrt[3]{2})$) ،

$$Aut(\mathbb{Q}(\sqrt[3]{2});\mathbb{Q}) = \{\varphi \in Aut\,\mathbb{Q}(\sqrt[3]{2}) : \varphi(a) = a \ \forall\, a \in \mathbb{Q}\}$$

وبالتالى فلكل $\varphi \in Aut(\mathbb{Q}(\sqrt[3]{2}))$:

$$2 = \varphi(2) = \varphi((\sqrt[3]{2})^3) = (\varphi(\sqrt[3]{2}))^3 \Rightarrow \varphi(\sqrt[3]{2}) = \sqrt[3]{2}, \varphi((\sqrt[3]{2})^2) = (\sqrt[3]{2})^2$$

(لأن $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ فينتج أن $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$)

ومن حيث إن $X^3 - 2$ لها فى $\mathbb{Q}(\sqrt[3]{2})$ الصفر الوحيد $\sqrt[3]{2}$ وهى كثيرة الحدود الصغرى من $\sqrt[3]{2}$ على $\mathbb{Q}$ فينتج أن $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ أساس للفراغ الخطى $\mathbb{Q}(\sqrt[3]{2})$ على الحقل $\mathbb{Q}$. (انظر (١-٥-٥)). ومن حيث إن φ ، 1 لهما نفس "القيم" عند عناصر أساس الفراغ الخطى ، فيكون $\varphi = 1$.

وهو المطلوب .

٢-٢-٤ نظرية جالوا الأساسية The Main Theorem of Galois

ليكن $K \subset k$ امتداد جالوا ، A مجموعة الحقول البينية فى $K \subset k$ ، B مجموعة الزمر الجزئية من $Aut(K;k)$. عندئذ فإن :

(١) الراسمان : $Aut(K;\ ) : A \to B, L \mapsto Aut(K;L),$

$$Fix(K;\ ) : B \to A, G \mapsto Fix(K;G)$$

تناظران أحاديان ، وكلاهما معكوس الآخر ، أى أن :

$Fix\,(K;\ Aut(K;L)) = L \qquad \forall L \in A,$

$Aut(K;\ Fix\,(K;G)) = G \qquad \forall G \in B$

(٢) لكل حقل بينى L فى $K \subset k$:

(أ) (رتبة الزمرة $Aut(K;L)$) $[K:L] = Ord\,(Aut(K;L))$

(ب) $[L:K] = [Aut(K;k) : Aut(K;L)]$

راجع تعريف الرتبة والدليل فى (١-١٠) من نظرية الزمر)

(٣) لكل حقل بينى L فى $K \subset k$:

(أ) $K \supset L$ امتداد جالوا

(ب) $Aut(K;L)$ زمرة جزئية طبيعية من $Aut(K;k)$ إذا كان وفقط إذا كان $L \supset k$ امتداد جالوا

(جـ) إذا كان $L \supset k$ امتداد جالوا ، فإن :

(١) $\varphi(L) = L$ لكل $\varphi \in Aut(K;k)$

(٢) الراسم

$$\begin{aligned} Aut(K;k) &\to Aut(L;k) \\ \varphi &\mapsto \varphi | L \end{aligned}$$

إبيمورفيزم

(٣) $Aut(L;k) \cong Aut(K;k) / Aut(K;L)$

٢-٢-٥ مثال :

يمكن البرهنة على أن $\mathbb{Q}(\sqrt{2},\sqrt{3}) \supset \mathbb{Q}$ هو امتداد جالوا بمعلومات ستأتى فيما بعد ، ولكننا نبرهن الآن على ذلك بمعلوماتنا الحالية ولهذا نعرف $K := \mathbb{Q}(\sqrt{2},\sqrt{3})$ ، ليكن $x \in Fix\,(K;Aut(K;\mathbb{Q}))$. عندئذ فإنه توجد $a,b,c,d \in \mathbb{Q}$ بحيث يكون $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$. وباستخدام معلوماتنا من المثال فى (٢-١-٥) فيكون لدينا $c\sqrt{3} + d\sqrt{2}\sqrt{3} = -c\sqrt{3} - d\sqrt{2}\sqrt{3}$ وبالتالى فإنه من $\varphi_1(x) = x$

يكون $c = d = 0$. ومن $\varphi_2(x) = x$ ينتج كذلك أن $b = 0$ ، وبهذا يكون $x \in \mathbb{Q}$.

أى أننا وجدنا G زمرة جزئية منتهية من $Aut(K)$ أى من $Aut(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ بحيث يكون $k = \mathbb{Q} = Fix(K,G)$ حيث G هى زمرة كلاين الرباعية ، وبهذا يكون $\mathbb{Q}(\sqrt{2},\sqrt{3}) \supset \mathbb{Q}$ امتداد جالوا. (G هى بالفعل $Aut(K)$ كما سبق أن رأينا فى (٢-١-٥))

والآن الزمر الجزئية الفعلية من $Aut(K) = Aut(K,\mathbb{Q})$ هى : $H_1 := \{1,\varphi_1\}$ ، $H_2 := \{1,\varphi_2\}$ ، $H_3 := \{1,\varphi_3\}$. وبالتالى يكون لامتداد الحقل $K \supset \mathbb{Q}$ بالضبط ثلاثة حقول بينية فعلية هى $L_i := Fix(K;H_i)$ حيث $i \in \{1,2,3\}$ ومن النظرية الأساسية لجالوا $Aut(K,L_i) = H_i$ ، $[K:L_i] = Ord(H_i) = 2$ لكل i . ولأن $\sqrt{2} \in L_1$ ، $\sqrt{3} \in L_2$ ، $\sqrt{2}\sqrt{3} \in L_3$ ينتج أن $\mathbb{Q}(\sqrt{2}) = L_1$ ، $\mathbb{Q}(\sqrt{3}) = L_2$ ، $\mathbb{Q}(\sqrt{2},\sqrt{3}) = L_3$.

ولأن الزمرة $Aut(K)$ إبدالية فإن الزمر الجزئية H_i زمر جزئية طبيعيـــة . وينـــتج كذلك من النظرية الأساسية لجالوا أن امتدادات الحقول $\mathbb{Q} \supset L_i$ هى امتدادات جـــالوا .

(يستطيع المرء بالطبع أن يثبت ذلك مباشرة)

<u>٢-٢-٦ تعريف</u> :

لتكن G زمرة ، K حقلاً ، $K^* := K \setminus \{0\}$ ، يسمى هومومورفيزم الزمر

$$\chi : G \to K^*$$

<u>رمز أو صفة</u> (character) G فى K

<u>٢-٢-٧ تمهيدية</u> :

الرموز المختلفة مثنى مثنى χ_1 ، ... ، χ_n لزمرة G فى حقل K تكون عناصر مستقلة خطياً للفراغ الخطى لكل رواسم G فى K على الحقل K

<u>البرهان</u> : بالاستقراء الرياضى على n :

عند $n=1$ يكون الادعاء صحيحاً لأنه إذا كان $\chi: G \to K^*$ رمزاً ، وكان e هو عنصر G المحايد فمن $\lambda\chi = 0$ حيث $\lambda \in K$ ينتج أن :

$$\lambda = \lambda 1 = \lambda(\chi(e)) = (\lambda\chi)(e) = 0(e) = 0_K \quad (\text{صفر الحقل } K)$$

(1 هو عنصر الوحدة فى K ، 0 هو صفر الفراغ الخطى)

والآن ليكن الادعاء صحيحاً لكل $n-1$ من الرموز المختلفة مثنى مثنى لـــ G فى K .

فإذا كات χ_1 ، ... ، χ_n رموزاً مختلفة مثنى مثنى لـــ G فى K ، فإنه يوجد $a \in G$ بحيث يكون $\chi_1(a) \neq \chi_n(a)$. ومن :

$$\lambda_1\chi_1 + \ldots + \lambda_n\chi_n = 0 \qquad (1)$$

حيث λ_1، ... ، λ_n عناصر فى K نحصل على المتساويتين الآتيتين لكل $g \in G$:

$$\lambda_1\chi_1(a)\chi_1(g) + \ldots + \lambda_n\chi_n(a)\chi_n(g) = 0,$$
$$\lambda_1\chi_n(a)\chi_1(g) + \ldots + \lambda_n\chi_n(a)\chi_n(g) = 0$$

حيث حصلنا على الأولى بتأثير الصيغة (1) على ag ، وعلى الثانية بالتأثير بالصيغة (1) على g ، والضرب فى $\chi_n(a)$. وبالطرح نحصل على :

$$\lambda_1(\chi_1(a) - \chi_n(a))\chi_1(g) + \ldots + \lambda_{n-1}(\chi_{n-1}(a) - \chi_n(a))\chi_{n-1}(g) = 0$$

لكل $g \in G$. ومن فرض الاستقراء، وعلى وجه الخصوص فإن $\lambda_1(\chi_1(a) - \chi_n(a)) = 0$.

ولأن $\chi_1(a) \neq \chi_n(a)$ فإن $\lambda_1 = 0$. وباستخدام فرض الادعاء مرة اخرى على (1) نحصل على $\lambda_2 = \ldots = \lambda_n = 0$.

والآن نحتاج إلى النتيجة الآتية :

<u>**٢-٢-٨ نتيجة**</u> : إذا كانت φ_1 ، ... ، φ_n مونومورفيزمات حقل K إلى حقل K' ، مختلفة مثنى مثنى ، فإن φ_1 ، ... ، φ_n تكون مستقلة خطياً فى الفراغ الخطى لجميع الرواسم من K إلى K' على الحقل K' .

٢-٢-٩ تمهيدية :

لتكن φ_1 ، ... ، φ_n مونومورفيزمات حقل K إلى حقل K' ، مختلفة مثنى مثنى ، ولتكن $L := \{x \in K \mid \varphi_1(x) = ... = \varphi_n(x)\}$. فإن :

(١) L حقل جزئى من K

(٢) $[K:L] \geq n$

البرهان :

(١) إذا كان 1 عنصر الوحدة فى K فإن $\varphi_1(1) = ... = \varphi_n(1) = 1'$ حيث $1'$ عنصر الوحدة فى K' .

أى أن $1 \in L$ ، أى أن $L \neq \phi$ (انظر مثال ٢٣ فى (١-٢-٨) – نظرية الحلقات).

والآن ليكن $a \in L$ ، $b \in L$ فإن :

$$\varphi_1(a-b) = \varphi_1(a) - \varphi_1(b) = ... = \varphi_n(a) - \varphi_n(b) = \varphi_n(a-b)$$

أى أن $a-b \in L$ ، والآن لجميع $a \in L$ ، $b \in L \setminus \{0\}$

$$\varphi_1(ab^{-1}) = \varphi_1(a)\varphi_1(b^{-1}) = \varphi_1(a)\varphi_1(b)^{-1} = ... = \varphi_n(a)\varphi_n(b)^{-1}$$
$$= \varphi_n(a)\varphi_n(b^{-1}) = \varphi_n(ab^{-1})$$

أى أن $ab^{-1} \in L$

(٢) لنفترض أن $r := [K:L] < n$ ، ولنختر أساساً a_1 ، ... ، a_r للفراغ الخطى K على L . ولأن $r < n$ فإن المعادلات الخطية المتجانسة على K' :

$$\left.\begin{array}{c} \varphi_1(a_1)X_1 + ... + \varphi_n(a_1)X_n = 0 \\ \vdots \qquad\qquad \vdots \\ \varphi_1(a_r)X_1 + ... + \varphi_n(a_r)X_n = 0 \end{array}\right\} \qquad \#$$

لها حل غير تافه $(x_1,...,x_n) \in (K')^n$. لكل $a \in K$ يوجد $\lambda_1,...,\lambda_r \in L$ بحيث إن $a = \lambda_1 a_1 + ... + \lambda_r a_r$ ، ولأن $\varphi_i(\lambda_j) = \varphi_1(\lambda_j)$ لجميع $i \in \{1,...,n\}$ ، $j \in \{1,...,r\}$ (*) ، فإننا نحصل على :

$$\sum_{i=1}^{n} x_i\varphi_i(a) = x_1\varphi_1(a)+\ldots+x_n\varphi_n(a)$$

$$= x_1\varphi_1(\lambda_1 a_1+\ldots+\lambda_r a_r)+\ldots+x_n\varphi_n(\lambda_1 a_1+\ldots+\lambda_r a_r)$$

$$= x_1[\varphi_1(\lambda_1)\varphi_1(a_1)+\ldots+\varphi_1(\lambda_r)\varphi_1(a_r)]+\ldots$$

$$+x_n[\varphi_n(\lambda_1)\varphi_n(a_1)+\ldots+\varphi_n(\lambda_r)\varphi_n(a_r)]$$

$$\underset{(*)}{=}\varphi_1(\lambda_1)[x_1\varphi_1(a_1)+\ldots+x_n\varphi_n(a_1)]+\ldots$$

$$+\varphi_1(\lambda_r)[x_1\varphi_1(a_r)+\ldots+x_n\varphi_n(a_r)]=0$$

(لأن $(x_1,\ldots,x_n)\in(K')^n$ حقل للنظام #)

وبالتالى فإن $x_1\varphi_1+\ldots+x_n\varphi_n=0$ حيث $(x_1,\ldots,x_n)\neq(0,\ldots,0)$ وهذا تناقض مع (٢-٢-٨).

نهاية البرهان .

وفى حالة أن يكون L الحقل الثابت لزمرة منتهية من أوتومورفيزمات K ، نريد أن نقدر $[K:L]$ ، ولهذا سنتخذ مفاهيم أخرى مساعدة .

<u>٢-٢-١٠ تعريف</u> :

ليكن K حقلاً ، G زمرة جزئية منتهية من $Aut(K)$. يسمى الراسم

$$Tr_G : K\to K, a\mapsto \sum_{\varphi\in G}\varphi(a)$$

<u>أثر</u> (trace) G فى K

<u>٢-٢-١١ تمهيدية</u> :

ليكن K حقلاً ، ولتكن G زمرة جزئية منتهية من $Aut(K)$. عندئذ فإن :

$$\{0\}\neq Tr_G(K)\subset Fix(K;G)$$

<u>البرهان</u> : لكل $\psi\in G$ يكون النقل الأيسر $\begin{matrix} G\to G \\ \varphi\mapsto\psi o\varphi\end{matrix}$ تناظراً أحادياً (لأنه يوجد الراسم العكسى له $\begin{matrix} G\to G \\ \varphi\mapsto\psi^{-1}o\varphi\end{matrix}$ ، ψ^{-1} معرف لأن ψ أوتومورفيزم) ، وبهذا يكون لكل $a\in K$:

$$\psi(\sum_{\varphi\in G} \varphi(a)) = \sum_{\varphi\in G} \psi(\varphi(a)) = \sum_{\varphi\in G} \varphi(a)$$

النقل تناظر أحادى ψ هومومورفيزم

وهذا يعنى أن

$$Tr_G(K) \subset Fix(K;G)$$

وبافتراض أن $Tr_G(K)=\{0\}$ ينتج أنه لجميع $a\in K$: $\sum_{\varphi\in G} \varphi(a)=0$ أى أن

$\sum_{\varphi\in G} \varphi=\hat{0}$ حيث $\hat{0}$ الراسم الصفرى – هذا يعنى أن عناصر G مرتبطة خطياً :

تناقض مع (٢-٢-٨)

<u>٢-٢-١٢ تمهيدية</u> :

ليكن K حقلاً ، ولتكن G زمرة جزئية منتهية من $Aut(K)$. عندئذ فإن :

$$[K:Fix(K;G)]=Ord(G)$$

<u>البرهان</u> : من (٢-٢-٩) يكفى أن نبرهن على أن $[K:Fix(K;G)]\le Ord(G)$.

إذا كان $Ord(G)=n$ ، $G=\{\varphi_1,...,\varphi_n\}$ فيكون المطلوب هو البرهنة على أن لكل $m>n$ كل m من العناصر : $a_1,...,a_m\in K$ تكون مرتبطة خطياً على $Fix(K;G)$. ولأن $m>n$ يكون لنظام المعادلات المتجانسة

$$\begin{aligned}
\varphi_1^{-1}(a_1)X_1+...+\varphi_1^{-1}(a_m)X_m &= 0\\
\vdots \qquad\qquad\qquad \vdots \qquad\quad &\ \ \vdots\\
\varphi_n^{-1}(a_1)X_1+...+\varphi_n^{-1}(a_m)X_m &= 0
\end{aligned}$$

حل غير صفرى

ونظراً لأن أى مضاعف لأى حل يكون حلاً كذلك ولأن $Tr_G(K)\ne\{0\}$ فإنه يوجد حل $(x_1,...,x_m)\in K^m$ بحيث يكون

$$Tr_G(x_\ell)=\varphi_1(x_\ell)+...+\varphi_n(x_\ell)\ne 0$$

لواحدة ℓ : $\ell \in \{1,...,m\}$

ولأن $(x_1,...,x_m)$ حل لنظام المعادلات فإنه ينتج أن :

$$a_1\varphi_1(x_1)+...+a_m\varphi_1(x_m)=0$$
$$\vdots \qquad\qquad \vdots$$
$$a_1\varphi_n(x_1)+...+a_m\varphi_n(x_m)=0$$

وبالجمع نحصل على :

$$a_1(\varphi_1(x_1)+...+\varphi_n(x_1))+...+a_m(\varphi_1(x_m)+...+\varphi_n(x_m))=0$$

أى أن :

$$\sum_{j=1}^{m} a_j \sum_{i=1}^{n} \varphi_i(x_j)=0$$

بعبارة أخرى ، فإن : $\sum_{j=1}^{m} Tr_G(x_j)a_j=0$

ولأن $Tr_G(x_j)\neq 0$ ، فإن العناصر a_1 ، ... ، a_m تكون مرتبطة خطياً على $Tr_G(K)$ وبالتالى على $Fix(K;G)$ (٢-٢-١١) نهاية البرهان .

<u>٢-٢-١٣ تمهيدية</u> :

ليكن K حقلاً ، ولتكن G زمرة جزئية منتهية من $Aut(K)$. عندئذ فإن :

$$Aut(K;Fix(K;G))=G$$

<u>البرهان</u> :

$$Aut(K;Fix(K;G))=\{\varphi\in Aut(K)\mid \varphi(a)=a \quad \forall a\in Fix(K;G)\}$$

ومن ثم فإن $Aut(K;Fix(K;G))\supset G$

نبرهن الآن على "$\subset$" :

ليكن $\varphi\in Aut(K;Fix(K;G))$ ، $\varphi\notin G$. ولتكن رتبة G هى n ، وعناصرها φ_1 ، ... ، φ_n ، حيث $\varphi_1=1_K$ ، والآن :

$$Fix(K;G)=\{a\in K \mid a=\varphi_2(a)=...=\varphi_n(a)\}$$
$$=\{a\in K \mid \varphi(a)=a=\varphi_2(a)=...=\varphi_n(a)\}$$
$$=\{a\in K \mid \varphi(a)=\varphi_1(a)=\varphi_2(a)=...=\varphi_n(a)\}$$

ومن (٢-٢-٩) ينتج أن $[K:Fix(K;G)]\geq n+1$: تناقض مع (٢-٢-١٢) .

<u>٢-٢-١٤ استنتاج</u> :

ليكن $K\supset k$ امتداد جالوا ، H زمرة جزئية منتهية من $Aut(K)$، $k=Fix(K;H)$.

عندئذ فإن

(١) $H=Aut(K;k)$

(٢) $Aut(K;Fix(K;G))=G$ لكل G زمرة جزئية من $Aut(K;k)$

<u>البرهان</u> : (١) تنتج من (٢-٢-١٣) مباشرة ، ومن ذلك ينتج أن كل زمرة جزئية من $Aut(K;k)$ تكون منتهية . (٢) تنتج كذلك من (٢-٢-١٣) .

<u>٢-٢-١٥ تمهيدية</u> :

ليكن $K\supset L$ امتداد حقل . التقريرات الآتية متكافئة :

(١) $K\supset L$ امتداد جالوا

(٢) $[K:L]=Ord(Aut(K;L))<\infty$

(٣) $Ord(Aut(K;L))<\infty, Fix(K;Aut(K;L))=L$

<u>البرهان</u> : " (١) $\Leftarrow$ (٢)" : ينتج من (٢-٢-١٢) ، (٢-٢-١٤) (ضع $L=Fix(K;G)$)

"(٢) $\Leftarrow$ (٣)" : نعرف $G:=Aut(K;L)$ فينتج أن : $L\subset Fix(K;G)\subset K$

من (٢) ، (٢-٢-١٢) ينتج أن $[K:Fix(K;G)]=Ord(G)=[K:L]$ ونحصل على $L=Fix(K;G)$

"(٣) $\Leftarrow$ (١)" : واضح

<u>٢-٢-١٦ تمهيدية</u> :

ليكن L حقلاً بينياً فى امتداد جالوا $K\supset k$. ينتج أن $K\supset L$ امتداد جالوا

البرهان : نعرف $G := Aut(K;k)$ ومن ثم فإن $Ord(G) < \infty$ ، $Fix(K;G) = k$ (انظر (٢-٢-١٥)) . نعرف $H := Aut(K;L)$ ، $L' := Fix(K;H)$. ولأن $Aut(K;L)$ زمرة جزئية منتهية من $Aut(K)$ فيتبقى فقط أن نثبت أن : $L = L'$. من حيث إن $L' = Fix(K;Aut(K;L))$ ، $Aut(K;L) := \{\varphi \in Aut(K) \mid \varphi(a) = a \quad \forall a \in L\}$ فينتج مباشرة أن $L \subset L'$. والآن لجميع $\varphi, \varphi' \in G$ يكون

$$\varphi' o \varphi^{-1} \in Aut(K;L) = H \Leftrightarrow (\varphi' o \varphi^{-1})(a) = a \quad \forall a \in L$$
$$\Leftrightarrow \varphi'(a) = \varphi(a) \quad \forall a \in L \Leftrightarrow \varphi' | L = \varphi | L$$

إذا كان $r := [G:H]$ فإنه يوجد $\varphi_1, \ldots, \varphi_r \in G$ بحيث تكون التحديدات :

$$\psi_i := \varphi_i \mid L : L \to K, i \in \{1, \ldots, r\}$$

مونومورفيزمات مختلفة مثنى مثنى

ولأن

$$\{a \in L : \psi_1(a) = \ldots = \psi_r(a)\} = L \cap Fix(K;G) = L \cap k = k$$

فينتج من (٢-٢-٩) أن : $[L:k] \geq r$.

ومن

$$[K:k] = Ord(G) = [G:H].Ord(H) = r.[K:L'] \quad (١)$$

(لأن $L' = Fix(K;H)$)

ومن $K \supset L' \supset L \supset k$ ينتج أن

$$[K:k] = [K:L][L:k] \geq [K:L].r \quad (٢)$$

من (١) ، (٢) ينتج أن :

$$[K:L'] \geq [K:L] = [K:L'][L':L]$$
$$\Rightarrow 1 \geq [L':L] \underset{L' \supset L}{\Rightarrow} L' = L$$

نهاية البرهان .

٢-٢-١٧ تمهيدية :

ليكن L حقلاً بينياً فى امتداد الحقل $K \supset k$. عندئذ فإنه لكل $\varphi \in Aut(K;k)$ يكون :

$$Aut(K;\varphi(L)) = \varphi o Aut(K;L) o \varphi^{-1}$$

البرهان :

$$\psi \in Aut(K;\varphi(L)) \Leftrightarrow \psi(\varphi(a)) = \varphi(a) \quad \forall a \in L$$

$$\Leftrightarrow \varphi^{-1}(\psi(\varphi(a))) = a \quad \forall a \in L \Leftrightarrow \varphi^{-1} o \psi o \varphi \in Aut(K;L)$$

$$\Leftrightarrow \psi \in \varphi o Aut(K;L) o \varphi^{-1}$$

٢-٢-١٨ تمهيدية :

ليكن $K \supset k$ امتداد جالوا . إذا كان L حقلاً بينياً فى $K \supset k$ ، وكان $\varphi(L) = L$ لجميع $\varphi \in Aut(K;k)$ فإن الراسم

$$Aut(K;k) \to Aut(L;k)$$
$$\varphi \mapsto \varphi | L$$

إبيمورفيزم ، نواته هى $Aut(K;L)$

البرهان : من الواضح تماماً أن الراسم هومومورفيزم . كذلك فإن نواته تعطى بـــ :

$$\{\varphi \in Aut(K;k) \mid \varphi | L = 1_{Aut(L;k)}\}$$
$$= Aut(K;L)$$

ونبرهن الآن على أن هذا الراسم غامر (شامل ، فوقى) كالآتى :

ليكن صورة الراسم هى $G \subset Aut(L;k)$. لأن $K \supset k$ هو امتداد جالوا فإن

$$Fix(L;G) = k$$

G كصورة زمرة منتهية (٢-٢-١٥) تكون كذلك منتهية . ومن (٢-٢-١٣) ينتج أن $G = Aut(L;k)$.

٢-٢-١٩ تمهيدية :

ليكن $K \supset k$ امتداد جالوا . وليكن L حقلاً بينياً فى $K \supset k$. التقريرات الآتية متكافئة :

(١) $L \supset k$ امتداد جالوا

(٢) لكل $\varphi \in Aut(K;k)$: $\varphi(L)=L$

(٣) $Aut(K;L)$ زمرة جزئية طبيعية من $Aut(K;k)$

البرهان :

"(١) $\Leftarrow$ (٢)" لتكن $H:=Aut(L;k)$ ، M مجموعة جميع المونومورفيزمات $\psi: L\to K$ بحيث يكون $\psi \mid k=1_k$. وبهذا يمكن اعتبار H مجموعة جزئية من M . لأن $L\supset k$ امتداد جالوا يكون $Fix(L;H)=k$ ، ومن (٢-٢-٩) يكون $H=M$.ولكل $\varphi\in Aut(K;k)$ يقع $\varphi \mid L: L\to K$ فى M ، وبالتالى فى H ، ونحصل على $\varphi(L)=L$

"(٢) $\Leftarrow$ (١)" : من (٢-٢-١٨) الراسم $\begin{matrix} Aut(K;k)\to Aut(L;k) \\ \varphi\mapsto\varphi\mid L\end{matrix}$ راسم غامر (شامل ، فوقى). ولأن $K\supset k$ امتداد جالوا ، فإن $Ord(Aut(K;k))$ يكون منتهياً أى أن $H:=Aut(L;k)$ تكون زمرة منتهية . ونحتاج فقط إلى البرهنة على أن $k=Fix(L,H)$.واضح أن $k\subset Fix(L;H)$. والآن إذا كان هناك $a\in Fix(L;H)\setminus k$ فإننا نستطيع أن نجد $\varphi\in Aut(K;k)$ بحيث يكون $\varphi(a)\neq a$. ولأن $K\supset k$ امتداد جالوا يكون من (٢-٢-١٥): $Fix(K;Aut(K;k))=k$. ولـــ $\psi:=\varphi\mid L$ سيكون $\psi(a)\neq a$: تناقض مع $a\in Fix(L;H)$.

"(٢) $\Leftarrow$ (٣)" : واضح من (٢-٢-١٨) لأن $Aut(K;L)$ نواة هومومورفيزم .

"(٣) $\Leftarrow$ (٢)" : من (٢-٢-١٧) $Aut(K;\varphi(L))=Aut(K;L)$ لكل $\varphi\in Aut(K;k)$ (تذكر تعريف الزمرة الجزئية الطبيعية)

ومن (١) فى (٢-٢-٤) النظرية الأساسية لجالوا :

$$Aut(K;-):A\to B, L\mapsto Aut(K;L)$$

حيث A مجموعة الحقول البينية فى امتداد جالوا $K\supset k$ تناظر أحادى فينتج أن $\varphi(L)=L$.

بهذا تتم البرهنة على نظرية جالوا الأساسية .

٢-٣ الامتدادات الطبيعية للحقول Normal Field Extensions

٢-٣-١ تعريف :

يقال لامتداد الحقل $K \supset k$ إنه **طبيعى** (normal) إذا تحقق :

(١) $K \supset k$ جبرى

(٢) كل كثيرة حدود f **غير قابلة للتبسيط (للتحليل)** فى $k[X]$ ، والتى لها صفر فى K تتشقق على K فى عوامل خطية

والشرط (٢) يعنى أنه لكل $a \in K$: كثيرة الحدود الصغرى لـ a على k تتشقق على K فى عوامل خطية .

٢-٣-٢ نظرية :

لأى امتداد حقل منته $K \supset k$ التقريرات الآتية متكافئة :

(١) $K \supset k$ طبيعى

(٢) $K \supset k$ حقل تشقيق لكثيرة حدود $f \in k[X]$

(٣) إذا كان $K' \supset K$ امتداد حقل ، وكان $\varphi : K \to K'$ مونومورفيزماً بحيث إن $\varphi | k = 1_k$ فإن $\varphi(K) \subset K$

البرهان :

"(١) $\Leftarrow$ (٢)" : لأن $K \supset k$ امتداد حقل منته فإنه من (١-٦-٢) توجد عناصر $a_1,...,a_n \in K$ جبرية على k بحيث إن $K = k(a_1,...,a_n)$. ولكل $i \in \{1,...,n\}$ تتشقق كثيرة الحدود الصغرى f_i لـ a_i على k فى عوامل خطية على Kبحيث يكون $K \supset k$ بسبب $K = k(a_1,...,a_n)$ هو حقل التشقيق لكثيرة الحدود $f = f_1 ... f_n \in k[X]$.

"(٢) $\Leftarrow$ (٣)" :

من (٢) ، (١-٨-٨) يوجد $f \in k[X]$ ، $a_1,...,a_n, b \in K$ بحيث يكون : $f = b(X - a_1)...(X - a_n)$ ، $K = k(a_1,...,a_n)$ وينتج كذلك أنه بوجود K' ، $\varphi : K \to K'$ المعطى فى (٣) بالخصائص المتطلبة ، يكون لدينا :

$$f(\varphi(a_i)) = \varphi(f(a_i)) = \varphi(0) = 0, \quad \forall i \in \{1,...,n\}$$

ونحصل على $\varphi(\{a_1,...,a_n\}) \subset \{a_1,...,a_n\}$. ولأن $K = k(a_1,...,a_n)$ ينتج مباشرة أن $\varphi(K) \subset K$

"(٣) $\Leftarrow$ (١)" : $K \supset k$ منته يستلزم أن $K \supset k$ جبرى .

والآن لتكن $f \in k[X]$ غير قابلة للتحليل (للتبسيط) ، ولها صفر $a \in K$. نختار $a_1,...,a_n \in K$ بحيث يكون $K = k(a, a_1,...,a_n)$ ، ولتكن f_i هى كثيرة الحدود الصغرى لـــ a_i على k لجميع i ، وبهذا يكون K حقلاً بينياً لحقل التشقيق $K' \supset k$ لـــ $g := f f_1 ... f_n$. f تتشقق على K' فى عوامل خطية . وإذا كان $b \in K'$ صفراً لـــ f ، فإنه يوجد (من ١-٨-٨) أوتومورفيزم ψ لـــ K' بحيث يكون $\psi(a) = b$ ، $\psi(x) = x$ لجميع $x \in k$. وبتطبيق الشرط (٣) على المونومورفيزم $\psi | K : K \to K'$ نحصل على $b = \psi(a) \in K$ ، وهكذا تتشقق f على K فى عوامل خطية .

<u>**٢-٣-٣ مثال**</u> :

لأن امتداد الحقل $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ هو حقل التشقيق لكثيرة الحدود $X^2 - 2 \in \mathbb{Q}[X]$ فهو امتداد طبيعى .

وامتداد الحقل $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2})$ هو حقل التشقيق لكثيرة الحدود $X^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$ فهو امتداد طبيعى .

أما امتداد الحقل $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ ليس امتداداً طبيعياً ، لأن كثيرة الحدود

$$X^4-2=(X^2-\sqrt{2})(X^2+\sqrt{2})=(X-\sqrt[4]{2})(X+\sqrt[4]{2})(X-i\sqrt[4]{2})(X+i\sqrt[4]{2})$$

هى كثيرة حدود غير قابلة للتحليل (للتبسيط) فى $\mathbb{Q}[X]$ ، لها صفر فى $\mathbb{Q}(\sqrt[4]{2})$ لكنها لا تتشقق على $\mathbb{Q}(\sqrt[4]{2})$ فى عوامل خطية

٢-٤ الامتدادات القابلة للانفصال للحقول Seperable Field Extensions

٢-٤-١ تعريف :

ليكن k حقلاً ، وليكن $k \subset K$ حقل التشقيق لكثيرة حدود ليست ثابتة $f \in k[X]$. وليكن $a \in K$. يسمى العدد الطبيعي

$$\mu(f;a) := \max\{n \in \mathbb{N} \ : \ K[X] \text{ فى } (X-a)^n \mid (\text{يقسم})\ f\}$$

تعددية f فى a .

ويقال إن a **صفر بسيط** (simple zero) لـــ f كان $\mu(f;a)=1$ وإذا كان $\mu(f;a)\geq 2$ فيقال إن a **صفر مكرر** (repeated zero) لـــ f

٢-٤-٢ تعريف :

(أ) ليكن k حقلاً . تسمى كثيرة الحدود غير الثابتة $f \in k[X]$ إنها **قابلة للانفصال** (separable) إذا كان كل عامل غير قابل للتبسيط من عوامل f له أصفار بسيطة فقط فى حقل تشقيقه .

(ب) ليكن $k \subset K$ امتداد حقل . وليكن $a \in K$ يقال إن $a \in K$ **قابل للانفصال** على k إذا كان a صفراً لكثيرة حدود قابلة للانفصال $f \in k[X]$.

(جـــ) يقال إن امتداد الحقل $k \subset K$ **قابل للانفصال** إذا كان كل $a \in K$ قابل للانفصال على k .

(د) يقال إن الحقل k **تام** أو **كامل** (perfect) إذا كانت كل كثيرة حدود ليست ثابتة فى $k[X]$ قابلة للانفصال .

وإذا كان $K \supset k$ امتداد حقل فإن العنصر $a \in K$ الجبرى على k سيكون قابلاً للانفصال إذا كانت وفقط إذا كانت كثيرة الحدود الصغرى لـ a على k قابلة للانفصال . وسنبرهن فيما بعد على أن كل حقل له المميز صفر يكون تاماً . وكذلك كل حقل منته يكون تاماً .

<u>٢-٤-٣ تعريف</u> :

لتكن $R[X]$ حلقة كثيرات الحدود على حلقة إبدالية لها عنصر الوحدة $1 \in R$

$$D : R[X] \to R[X]$$

الراسم :

$$\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=1}^{n} i a_i X^{i-1}$$

يسمى <u>التفاضل الشكلى</u>(formal differentiation)فى $R[X]$. وهو <u>المشتقة</u>(derivative) فى $R[X]$ ، أى أنه يحقق :

$$D(af + bg) = aD(f) + bD(g),$$
$$D(f.g) = f.D(g) + g.D(f)$$

لكل $f, g \in R[X]$ ، ولكل $a,b \in R$.

<u>٢-٤-٤ تمهيدية</u> :

ليكن k حقلاً ، وليكن $K \supset k$ حقل التشقيق لكثيرة حدود ليست ثابتة $f \in k[X]$.
لكل $a \in K$ يتحقق ما يأتى :

(١) $\mu(f;a) = 1 \Leftrightarrow f(a) = 0, (Df)(a) \neq 0$

(٢) $\mu(f;a) > 1 \Leftrightarrow f(a) = 0, (Df)(a) = 0$

<u>البرهان</u>: ليكن $r := \mu(f;a)$. عندئذ فإنه توجد $g \in K[X]$ بحيث يكون $f = (X-a)^r g$، $g(a) \neq 0$ ، ونحصل على :

$$D(f) = (X-a)^{r-1}(rg + (X-a)D(g))$$

وينتج الادعاءان مباشرة .

ويستطيع المرء أن يتحقق إذا ما كانت كثيرة حدود f على حقل k لها أصفار مكررة على K أم ليس لها ، حيث K حقل يحتوى k ، دون حساب الأصفار .

<u>٢-٤-٥ تمهيدية</u> :

ليكن k حقلاً ، ولتكن f كثيرة حدود غير ثابتة فى $k[X]$. التقريران الآتيان متكافئان :

(١) f لها أصفار مكررة فى K حقل فوقى للحقل k .

(٢) f ، $D(f)$ لهما فى $k[X]$ قاسم مشترك ليس ثابتاً .

<u>البرهان</u> :

"(١) $\Leftarrow$ (٢)" : ليكن $a \in K$ صفراً مكرراً لـــ f ، g هى كثيرة الحدود الصغرى من a على k. لأن $f(a)=0$ ، $(Df)(a)=0$ تكون g قاسماً مشتركاً لـــ f ، $D(f)$

"(٢) $\Leftarrow$ (١)" : لتكن $g \in k[X]$ قاسماً مشتركاً لـــ f ، $D(f)$ ، $\deg(g) \geq 1$ ، a صفراً لـــ g فى حقل فوقى لـــ k . عندئذ فإن $f(a)=0$ ، $(Df)(a)=0$ ويكون a صفراً مكرراً لـــ f.

<u>٢-٤-٦ نظرية</u> :

ليكن k حقلاً . كثيرة حدود $f \in k[X]$ <u>غير القابلة للتحليل (للتبسيط)</u> تكون قابلة للانفصال إذا كان وفقط إذا كان $D(f) \neq 0$

<u>البرهان</u> : إذا كان $D(f)=0$ فمن (٢-٤-٤) يكون كل صفر لـــ f فى حقل فوقى لـــ k مكرراً. وبالتالى تكون f قابلة للانفصال .

وإذا كان $D(f) \neq 0$ ، فإن f كون قابلة للانفصال وإلا فمن التعريف (٢-٤-٢ (أ)) ومن التمهيدية (٢-٤-٥) يكون لـــ f ، $D(f)$ فى $k[X]$ قاسم مشترك غير ثابت g .

ولأن f غير قابلة للتبسيط (أو التحليل) فإن هذا يؤدى إلى تناقض :

$$\deg(g) = \deg(f) > \deg(D(f))$$

<u>٢-٤-٧ تمهيدية</u> :

ليكن k حقلاً ، $f \in k[X]$.

إذا كان $Char(k)=0$ (مميز k) فإن

$D(f)=0 \Leftrightarrow f$ ثابت

إذا كان $Char(k)=p>0$ فإن :

$$D(f)=0 \Leftrightarrow \exists g \in k[X]: f(X)=g(X^p)$$

<u>البرهان</u> : فى حالة المميز = الصفر ينتج الادعاء مباشرة من تعريف D . والآن إذا كان $p := Char(k) > 0$ ، $f=\sum_{i=0}^{n} a_i X^i$ ، فإن $D(f)=0$ تعنى أنه لجميع $i \in \{1,\dots,n\}$ ، $a_i \neq 0$ تكون p قاسماً لـــ i ، وتكون f لها الشكل :

$$f = a_0 + a_p X^p + a_{2p} X^{2p} + \dots + a_{mp} X^{mp}$$

نهاية البرهان .

والآن من (٢-٤-٦) ، (٢-٤-٧) ينتج مباشرة :

<u>٢-٤-٨ استنتاج</u> :

كل حقل له المميز صفر يكون تاماً

سنرى فيما بعد أن كل حقل منته يكون كذلك تاماً . وللحصول على امتداد حقل جبرى وليس قابلاً للانفصال ، يجب علينا أن نبدأ بحقل غير منته ، ومميزه مختلف عن الصفر . وسنختار الحقل $k := (\mathbb{Z}/p\mathbb{Z})(X)$ على سبيل المثال ، حيث p عدد أولى . وهكذا فإن k هو حقل الدوال الكسرية فى غير محدد "X" على الحقل $\mathbb{Z}/p\mathbb{Z}$. والآن حقل التشقيق $K \supset k$ لكثيرة الحدود $Y^p - X \in k[Y]$ يحقق الخصائص المرجوة ، لأنه من (٣-٥-١٠) ، (٣-٦-٢) فى نظرية الحلقات تكون كثيرة الحدود $Y^p - X$ غير قابلة للتبسيط (للتحليل) فى $k[Y]$ ، ولأن $D(Y^p - X)=0$ فإنها تكون غير قابلة للانفصال (٢-٤-٦).

٢-٤-٩ ملحوظة :

ليكن $K \supset k$ امتداد حقل . وليكن $a \in K$ قابلاً للانفصال على k . ينتج أن a قابل للانفصال على أى حقل بينى L فى $K \supset k$

البرهان : كثيرة الحدود الصغرى لـــ a على L تقسم فى $L[X]$ كثيرة الحدود الصغرى لـــ a على k، وهذه الأخيرة قابلة للانفصال ، وبهذا تكون الأولى قابلة للانفصال. (نحن نعلم أن العنصر $a \in K$ الجبرى على k يكون قابلاً للانفصال إذا كانت وفقط إذا كانت كثيرة الحدود الصغرى لـــ a على k قابلة للانفصال) .

٢-٥ وصف (خصائص) امتدادات جالوا

Characterization of Galois Extensions

فيما سبق عرفنا امتداد جالوا $K \supset k$ من خلال الشرط أن k هو الحقل الثابت لزمرة جزئية منتهية من $Aut(K)$ فى K . وبناءً عليه برهنا نظرية جالوا الأساسية بمساعدة بعض أدوات الجبر الخطى . لكن من الناحية التطبيقية فإنه يكون من الأفضل والأسهل أن نتعرف بعض الشروط لاختبار إذا ما كان هذا الامتداد امتداد جالوا أم لا .

٢-٥-١ تمهيدية :

ليكن $K \supset k$ امتداد حقل ، $a_1,\dots,a_n \in K$ مختلفة مثنى مثنى . ولتكن $s_1,\dots,s_n \in k[X_1,\dots,X_n]$ مختارة بحيث يكون :

$$\underline{(X-a_1)\dots(X-a_n)} = X^n - s_1(a_1,\dots,a_n)X^{n-1} + \dots + (-1)^n s_n(a_1,\dots,a_n) \quad (1)$$

عندئذ فإن

$$\varphi(s_i(a_1,\dots,a_n)) = s_i(a_1,\dots,a_n)$$

لجميع الهومومورفيزمات $\varphi: K \to K$ التى تحقق

$$\varphi(\{a_1,\dots,a_n\}) = \{a_1,\dots,a_n\}, \qquad (2)$$

ولجميع $i \in \{1,\dots,n\}$

البرهان : لأن

$$X^{n}-s_{1}(\varphi(a_{1}),\dots,\varphi(a_{n}))X^{n-1}+\dots+(-1)^{n}s_{n}(\varphi(a_{1}),\dots,\varphi(a_{n}))$$

$$\underset{(1)}{=}(X-\varphi(a_{1}))\dots(X-\varphi(a_{n}))\underset{(2)}{=}\underline{(X-a_{1})\dots(X-a_{n})} \qquad (3)$$

ونحصل من (1) ، (3) وبمساواة المعاملات للقوى المختلفة لـــ X على :

$$s_{i}(a_{1},\dots,a_{n})=s_{i}(\varphi(a_{1}),\dots,\varphi(a_{n})) \qquad (4)$$

ومن (2) ينتج أن :

$$s_{i}(\varphi(a_{1}),\dots,\varphi(a_{n}))=\varphi(s_{i}(a_{1},\dots,a_{n})) \qquad (5)$$

من (4) ، (5) ينتج المطلوب مباشرة .

٢-٥-٢ تمهيدية :

ليكن $k \subset K$ امتداد جالوا ، وليكن $a\in K$. لتكن a_{1} ، ... ، a_{n} العناصر المختلفة فى $\{\varphi(a):\varphi\in Aut(K;k)\}$ عندئذ فإن : $f:=(X-a_{1})\dots(X-a_{n})$ تكون هى كثيرة الحدود الصغرى لـــ a على k .

البرهان : لكل $\psi\in Aut(K;k)$ إذا "دارت" φ بحيث مثلت جميع عناصر $Aut(K;k)$ فإن $\psi o\varphi$ "تدور" كذلك بحيث تمثل جميع عناصر $Aut(K;k)$ ، ومن ثم فإن :

$$(\psi o\varphi)(\{a_{1},\dots,a_{n}\})=\{a_{1},\dots,a_{n}\} \qquad (1)$$

ولكن

$$(\psi o\varphi)(\{a_{1},\dots,a_{n}\})=\psi(\varphi(\{a_{1},\dots,a_{n}\}))=\psi(\{a_{1},\dots,a_{n}\}) \qquad (2)$$

من (1) ، (2) ينتج أن :

$$\psi(\{a_{1},\dots,a_{n}\})=\{a_{1},\dots,a_{n}\}$$

لجميع $\psi\in Aut(K;k)$

والآن فمن (٢-٥-١) تقع جميع معاملات f فى $Fix(K;Aut(K,k))=k$ (لاحظ أن $k\subset K$ امتداد جالوا) .

ولأن f مطبعة ، a أحد أصفار f (لاحظ أن $1 \in Aut(K;k)$ وبهذا يكون $a = 1(a)$ أحد العناصر a_1 ، ... ، a_n) ، فإنه يتبقى فقط أن نثبت أن f غير قابلة للتبسيط (للتحليل) فى $k[X]$.

والآن ليكن $g, h \in k[X]$ بحيث يكون (3) $f = gh$ ، $g(a) = 0$. عندئذ فإنه لكل $i \in \{1, ..., n\}$ يوجد $\varphi \in Aut(K;k)$ بحيث يكون $a_i = \varphi(a)$ ، $g(a_i) = g(\varphi(a)) = \varphi(g(a)) = \varphi(0) = 0$. ولأن العناصر a_1 ، ... ، a_n مختلفة مثنى مثنى ينتج أن $f \mid g$ (f تقسم g) ، ومع (3) تكون $h \in k^*$ ، أى أن f غير قابلة للتبسيط (للتحليل) .

<u>٢-٥-٣ نظرية</u> :

ليكن $K \supset k$ امتداد حقل . التقريرات الآتية متكافئة :

(١) $K \supset k$ امتداد جالوا

(٢) امتداد الحقل $K \supset k$ منته ، طبيعى ، قابل للانفصال .

(٣) $K \supset k$ هو حقل تشقيق لكثيرة حدود قابلة للانفصال فى $k[X]$

<u>البرهان</u> :

"(١) $\Leftarrow$ (٢)" : من (٢-٢-١٥) كل امتدادات جالوا تكون منتهية . ومن (٢-٥-٢) تكون كثيرة الحدود الصغرى لكل عنصر $a \in K$ على k هى حاصل ضرب منته من عوامل خطية مختلفة فى $K[X]$. وبهذا يكون امتداد الحقل $K \supset k$ طبيعياً وقابلاً للانفصال .

"(٢) $\Leftarrow$ (٣)" : لأن امتداد الحقل $K \supset k$ منته ، طبيعى ، فإنه من النظرية (٢-٣-٢) يكون هو حقل تشقيق لكثيرة حدود $f \in k[X]$. والمطلوب أن نبرهن على أن f بالضرورة قابلة للانفصال . ليكن g عاملاً من عوامل f ، وغير قابل للتبسيط ، وليكن $a \in K$ صفراً لـــ g . وبهذا تكون g مساوية لكثيرة الحدود الصغرى لـــ a على k (فيما عدا أنها تساوى كثيرة الحدود الصغرى لـــ a مضروبة فى عامل ثابت). ولأن a قابل للانفصال على k فإن g تكون قابلة للانفصال ، وبالتالى تكون f قابلة للانفصال .

"(٣) $\Leftarrow$ (١)" : ليكن $K \supset k$ حقل التشقيق لكثيرة حدود قابلة للانفصال $f \in k[X]$. من $G := Aut(K;k)$ نحصل على $k \subset Fix(K;G)$ ، ومن (٢-٢-٩) ينتج أن :

$$Ord(G) \leq [K : Fix(K;G)] \leq [K : k] < \infty$$

أى أن G منتهية

والمطلوب البرهنة على أن $\qquad Fix(K;G) = k$

سنعتمد فى البرهان على "r" عدد أصفار f فى $K \setminus k$ ، وسنستخدم الاستقراء الرياضى:

عند $r = 0$ يكون $K = k$ ، ومن ثم فإن $Fix(K;G) = k$

والآن ليكن $r \geq 1$ ، $a \in K \setminus k$ صفراً لـــ f ، كثيرة الحدود الصغرى g لـــ a على k هى قاسم لـــ f فى $k[X]$. ضع $k' := k(a)$ ، وبالتالى فإن $K \supset k'$ هو حقل التشقيق لكثيرة الحدود القابلة للانفصال $f \in k'[X]$ ، التى لها $r - 1$ من الأصفار فى $K \setminus k'$. ومن فرض الاستقراء الرياضى فإن $K \supset k'$ هو امتداد جالوا ، بحيث إنه توجد G' زمرة جزئية منتهية من $Aut(K)$ بحيث يكون

$$G' = Aut(K;k') \subset G \quad ، \quad k' = Fix(K;G')$$

ليكن الآن $\qquad x \in Fix(K;G) \subset Fix(K;G') = k(a)$

إذا كان $n := \deg(g)$ فإنه من (١-٥-٥) توجد عناصر $c_0, ..., c_{n-1} \in k$ بحيث يكون :

$$x = c_{n-1}a^{n-1} + ... + c_0$$

إذا كانت $a = a_1$ ، a_2 ، ... ، a_n أصفاراً لـــ g فى K فمن (١-٨-٨) ينتج أنه لكل $i \in \{1, ..., n\}$ توجد $\varphi_i \in G$ بحيث إن $\varphi_i(a) = a_i$ ، ونحصل على :

$$x \underset{x \in Fix(K;G)}{=} \varphi_i(x) = \varphi_i(c_{n-1}a^{n-1} + ... + c_1 a + c_0)$$
$$= \varphi_i(c_{n-1})\varphi_i(a^{n-1}) + ... + \varphi_i(c_1)\varphi_i(a) + \varphi_i(c_0)$$
$$\underset{\varphi_i \in G = Aut(K;k)}{=} c_{n-1}a_i^{n-1} + ... + c_1 a_i + c_0 \quad \forall i$$

والآن كثيرة الحدود

$$h := c_{n-1}X^{n-1} + ... + c_1X + (c_0 - x) \in K[X]$$

لها من ثم الأصفار a_1 ، ... ، a_n . ولأن $\deg(h) \le n-1$ فإنه ينتج أن $h = 0$ ، ومن ثم فإن $x = c_0 \in k$. وبالتالى فإن

$$Fix(K;G) = k$$

من (٢-٤-٨) ، (٢-٥-٣) ينتج مباشرة :

٢-٥-٤ استنتاج :

إذا كان K حقلاً له المميز صفر ، فإن امتداد الحقل $K \supset k$ يكون امتداد جالوا إذا كان وفقط إذا كان $K \supset k$ حقل تشقيق كثيرة حدود فى $k[X]$.

٢-٥-٥ نظرية :

ليكن $K \supset k$ امتداد حقل . لتكن $a_1,...,a_n \in K$ عناصر قابلة للانفصال على k بحيث إن $K = k(a_1,...,a_n)$. عندئذ فإن :

(١) امتداد الحقل $K \supset k$ منته ، قابل للانفصال .

(٢) يوجد حقل فوقى $L \supset K$ بحيث يكون $L \supset k$ امتداد جالوا

البرهان : كون $K \supset k$ منتهياً ينتج من (١-٦-٢)

لكل $i \in \{1,...,n\}$ تكون كثيرة الحدود الصغرى f_i لـ a_i على k قابلة للانفصال بحيث إن كثيرة الحدود $f = f_1..f_n \in k[X]$ تكون قابلة للانفصال . وإذا كان $L \supset K$ حقل تشقيق لـ f، فإن $L \supset k$ أيضاً سيكون حقل تشقيق لـ f لأن $K = k(a_1,...,a_n)$. ومن (٢-٥-٣) يكون $L \supset k$ امتداد جالوا ، ومن ثم فهو أيضاً قابل للانفصال . عندئذ فإن $K \supset k$ أيضاً قابل للانفصال .

٦-٢ تطبيق : الحقول المنتهية Finite Fields

٢-٦-١ ملحوظة :

إذا كان K حقلاً منتهياً ، P حقله الأولى (انظر (١-١-٨)) فإن :

$$Ord(K) = (Char(K))^{[K:P]}$$

البرهان : لأن K منته فإن $n := [K:P]$ تكون منتهية .

الفراغ الخطى K على الحقل P ذو البعد n يكون متشاكلاً (أيزومورفياً) مع P^n بحيث إن :

$$Ord(K) = (Ord(P))^n \quad = \quad (Char(K))^n$$

١-١-٩

سنذكر الآن نظرية بدون برهان :

٢-٦-٢ نظرية :

ليكن K حقلاً . كل زمرة جزئية منتهية من K^* تكون دائرية .

من النظرية السابقة مباشرة ، ومن (١-١١-٩) فى نظرية الزمر لدينا :

٢-٦-٣ استنتاج :

ليكن K حقلاً منتهياً يتكون من q من العناصر . عندئذ فإن :

(١) K^* دائرية

(٢) يوجد $a \in K$ بحيث يكون $K = \{0,1,a,...,a^{q-2}\}$

(٣) كل عنصر فى K يكون صفراً لكثيرة الحدود $X^q - X \in K[X]$

البرهان :

(١) من حيث إن K منته ، إذن K^* منته، K^* تكون زمرة جزئية منتهية من K^* ، وبالتالى فهى دائرية .

(٢) $K = K^* \cup \{0\}$ ، من حيث إن K^* دائرية ، وعدد عناصرها $q-1$ فيكون لها مولد a ، ويكون $K = \{0,1,a,...,a^{q-2}\}$

(٣) من (١-١١-٩) فى نظرية الزمر (نظرية كلاين - فرمات)

$$\forall\ b \in K^* \ :\ b^{q-1} = 1 \in K^*$$

وبالتالى فإن :

$$\forall\ b \in K^* \ :\ b^q - b = b^{q-1}b - b = 1b - b = 0$$

أى أن b صفر لكثيرة الحدود $X^q - X \in K[X]$. وواضح أن 0 صفر لكثيرة الحدود $X^q - X \in K[X]$. أى أن جميع عناصر K أصفار لكثيرة الحدود المعنية .

<u>٢-٦-٤ ملحوظة</u> :

ليكن K حقلاً له المميز $p > 0$ ، عندئذ فإن الراسم :

$$K \to K$$
$$x \mapsto x^p$$

مونومورفيزم . يسمى **<u>هومومورفيزم فوربينيس</u>** لـــ K .

(Forbenius – Homomorphism of K)

<u>البرهان</u> :

$$\forall\ x, y \in K : (\mathrm{xy})^p = \underbrace{(xy)...(xy)}_{p \text{ من المرات}} = \underbrace{(x)...(x)}_{p \text{ من المرات}}\underbrace{(y)...(y)}_{p \text{ من المرات}} = x^p y^p$$

والآن

$$(x+y)^p = x^p + ... + \binom{p}{r} x^{p-r} y^r + ... + y^p$$

العدد العام فى المفكوك هو

$$\binom{p}{r} x^{p-r} y^r = \frac{p!}{r!(p-r)!} x^{p-r} y^r$$

لاحظ أن $p \mid p!$ (p يقسم $p!$) بينما $p \nmid r!$ ، $p \nmid (p-r)!$ (لأن لجميع $1 \le r < p$: $p \nmid r$ ، $p \nmid p-r$) ومن حيث إن مميز الحقل هو p فإن

$$(x+y)^p = x^p + y^p$$

(راجع مثال (٣-٦-٧) ، مثال ١٥ فى (٣-٦-٩) فى نظرية الحلقات) (كذلك فإن : $1^p = 1$. أى أن الراسم هومومورفيزم)

ونثبت كذلك أنه راسم أحادى :

ليكن $x^p = y^p$. هذا يقتضى أن $x^p - y^p = 0$. ولكن

$$(x-y)^p = x^p - \binom{p}{1} x^{p-1} y + \ldots + (-1)^r \binom{p}{r} x^{p-r} y^r + \ldots + (-1)^p y^p$$

كما سبق يكون لدينا :

$$(x-y)^p = x^p + (-1)^p y^p$$

p عدد أولى : إذن $p = 2$ أو p عدد فردى .

إذا كان $p = 2$ فإن :

$$(x-y)^p = x^p + y^p = x^p - y^p$$

وإذا كان p عدداً فردياً فكذلك يكون لدينا :

$$(x-y)^p = x^p - y^p$$

أى أن $x^p = y^p$ ينتج عنه دائماً أن $(x-y)^p = 0$ ، وبالتالى فإن $x - y = 0$ (لأن الحقل ليس له قواسم صفرية) ، وبالتالى فإن $x = y$ ، ويكون الراسم أحادياً .

ومن ثم فالراسم المعطى مونومورفيزم .

<u>٢-٦-٥ ملحوظة :</u>

(١) هومومورفيزم فوربينيس لحقل منته هو أوتومورفيزم

(٢) لكل عدد أولى p هومومورفيزم فوربينيس للحقل $\mathbb{Z}/p\mathbb{Z}$ هو راسم الوحدة

البرهان :

(١) واضح لأن كل راسم أحادى (واحد لواحد) من مجموعة منتهية إلى نفسها يكون راسماً غامراً (شاملاً ، فوقياً) وبهذا يكون تناظراً أحادياً ويكون هومومورفيزم فوربينيس ليس مجرد مونومورفيزم ، بل هو فى هذه الحالة أوتومورفيزم .

(٢) $\mathbb{Z}/p\mathbb{Z}$ حقل منته ، عدد عناصره p : فمن (٢-٦-٣ (٣)) يكون :

$$\forall x \in \mathbb{Z}/p\mathbb{Z} : x^p = x$$

وبالتالى فإن هومومورفيزم – فوربينيس للحقل $\mathbb{Z}/p\mathbb{Z}$ هو الراسم

$$\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$
$$x \mapsto x$$

أى راسم الوحدة .

٢-٦-٦ نظرية :

أى حقل له المميز $p > 0$ يكون تاماً إذا كان وفقط إذا كان هومومورفيزم فوربينيس الخاص به غامراً (شاملاً ، فوقياً)

البرهان : ليكن K حقلاً له المميز $p > 0$.

إذا كان K تاماً ، فإنه يكون لكل $a \in K$ كثيرة الحدود $f := X^p - a \in K[X]$ قابلة للانفصال. ليكن $g \in K[X]$ عاملاً لـــ f غير قابل للتحليل (للتبسيط) ، $L \supset K$ حقل تشقيقه ، $b \in L$ صفر لـــ g . عندئذ فإن b يكون كذلك صفراً لـــ f ، أى أن $b^p = a$ ، وتكون – كما سبق – $f := X^p - b^p = (X - b)^p \in L[X]$ ، بحيث إنه يوجد $n \in \{1,\ldots,p\}$ بحيث يكون $g = (X - b)^n$. ولأن f قابلة للانفصال فإن g يجب أن يكون لها فقط أصفار بسيطة فى L ، ومن ثم فإن $n = 1$ ، $b \in K$. أى أنه لكل $a \in K$ يوجد $b \in K$ بحيث يكون $b^p = a$ ، أى أن هومومورفيزم–فوربينيس له يكون غامراً (شاملاً ، فوقياً).

والآن ليكن هومومورفيزم فوربينيس لـ K غامراً (شاملاً ، فوقياً) ، ولتكن $f \in K[X]$ غير قابلة للتحليل (للتبسيط) . إذا كان لـ f أصفار مكررة فى حقل تشقيقها ، فإنه توجد $g \in K[X]$ بحيث يكون $f(X) = g(X^p)$ (انظر (٢-٤-٧)) . وبالتالى فإنه يكون لدينا $a_0, \ldots, a_n \in K$ بحيث يكون $f(X) = a_0 + a_1 X^p + \ldots + a_n (X^p)^n$.

ومن الفرض فإنه لكل $i \in \{0, \ldots, n\}$ يوجد $b_i \in K$ بحيث يكون $b_i^p = a_i$. ومن ثم نحصل على :

$$
\begin{aligned}
f(X) &= b_0^p + b_1^p X^p + \ldots + b_n^p (X^n)^p \\
&= (b_0 + b_1 X + \ldots + b_n X^n)^p
\end{aligned}
$$

(مميز الحقل $p > 0$)

أى أن f لن تكون غير قابلة للتبسيط (للتحليل) : وهذا تناقض مع اختيار f . وبالتالى فإن f ليس لها أصفار مكررة فى حقل تشقيقها ، أى أنها قابلة للانفصال ، ويكون الحقل K تاماً .

<u>٢-٦-٧ استنتاج</u> :

كل حقل منته يكون تاماً

<u>البرهان</u> : ينتج مباشرة من (٢-٦-٥) ، (٢-٦-٦)

<u>٢-٦-٨ نظرية</u> :

لكل عدد أولى p ، ولكل $n \in \mathbb{N} \setminus \{0\}$:

(١) إذا كان $K \supset \mathbb{Z}/p\mathbb{Z}$ حقل تشقيق كثيرة الحدود $X^{p^n} - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ فإن K يكون حقلاً ذا p^n من العناصر

(٢) إذا كان K حقلاً ذا p^n من العناصر ، P هو حقله الأولى ، فإن $K \supset P$ يكون حقل تشقيق كثيرة الحدود $X^{p^n} - X \in P[X]$

(٣) كل حقلين يتكونان من p^n من العناصر يكونان متشاكلين .

البرهان :

(١) نبرهن أولاً على أن مجموعة أصفار كثيرة الحدود $f := X^{p^n} - X$ فى K تكون حقلاً بينياً فى $K \supset \mathbb{Z}/p\mathbb{Z}$ ، بحيث إن K تنطبق مع هذه المجموعة .

لأن الزمرة $(\mathbb{Z}/p\mathbb{Z})^*$ من الرتبة $p-1$ ، فإن $a^{p-1} = 1$ ، وبالتالى فإن $a^p = a$ ، وكذلك $a^{p^n} = a$ لجميع $a \in (\mathbb{Z}/p\mathbb{Z})^*$ ، بحيث إن $\mathbb{Z}/p\mathbb{Z}$ يكون محتوى فى مجموعة أصفار كثيرة الحدود f : $\forall a \in (\mathbb{Z}/p\mathbb{Z})^* : f(a) = a^{p^n} - a = a - a = 0$.

إذا كان a ، b صفرين لـ f فإننا نحصل على :

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b ,$$

$$(\frac{a}{b})^{p^n} = \frac{a^{p^n}}{b^{p^n}} = \frac{a}{b}, b \neq 0$$

أى أن $a \pm b$ ، $a \, . \, b$ ، $\frac{a}{b}$ إذا كان $b \neq 0$ أصفار لكثيرة الحدود f ، أى أن أصفار كثيرة الحدود تكون حقلاً جزئياً من K .

ومما سبق فإنها تكون حقلاً جزئياً بينياً فى $K \supset \mathbb{Z}/p\mathbb{Z}$ ، كذلك فإن كل عنصر فى K يكون صفراً لـ f .

ولأن $D(f) = -1 \neq 0$ فإن f يكون لها أصفاربسيطة فقط فى K (انظر (٢-٤-٤)) ، وبالتالى فإن K تتكون فقط من p^n عنصراً بالضبط هى أصفار كثيرة الحدود $f = X^{p^n} - X$.

(٢) لأن الزمرة K^* من الرتبة $p^n - 1$ فإن $a^{p^n} = a$ لجميع $a \in K^*$ ، ومن ثم فإن هذا أيضا لجميع $a \in K$. ولأن كثيرة الحدود $X^{p^n} - X$ لها على الأكثر

p^n من الأصفار فى حقل فوقى لـــ P ، فإن K هى مجموعة أصفار كثيرة الحدود فى حقل التشقيق . ومن ثم فإن $K \supset P$ هو حقل تشقيق كثيرة الحدود هذه .

(٣) ليكن K ، K' حقلين يتكون كل منهما من p^n من العناصر . من (٢-٦-١) $Char(K) = p = Char(K')$ ، بحيث إن P الحقل الأولى لـــ K يكون متشاكلاً مع P' الحقل الأولى لـــ K' (انظر (١-١-٩)) . من (٢) ومن (١-٨-٦) يكون K ، K' متشاكلين .

٢-٦-٩ تعريف :

إذا كان $n \neq 0$ عدداً طبيعياً ، p عدداً أولياً فيقال للحقل الوحيد – بدون حساب الأيزومورفيزمات– الذى يتكون من p^nمن العناصر إنه **حقل جالوا ذو p^n من العناصر**

(Galois field of p^n elements)

ويشار إليه بالرمز $GF(p^n)$.

٢-٦-١٠ نظرية :

ليكن $n \neq 0$ عدداً طبيعياً ، p عدداً أوليا . لكل حقل K يتكون من p^n من العناصر ، وحقله الأولى P :

(١) امتداد الحقل $K \supset P$ هو امتداد جالوا

(٢) هومومورفيزم فوربينيس لـــ K يولد زمرة أوتومورفيزمات K (التى تتطابق مع زمرة جالوا لـــ $K \supset P$ حسب (٢-١-٣))

البرهان :

(١) $D(X^{p^n} - X) = -1 \neq 0$ يقتضى أن كثيرة الحدود $X^{p^n} - X \in P[X]$ قابلة للانفصال ، فينتج من (٢-٦-٨) ، (٢-٥-٣) الادعاء مباشرة .

(٢) نحصل من النظرية الأساسية لجالوا(٢-٢-٤) ، ومن (٢-١-٣) على :

$$Ord(Aut(K)) \underset{\text{٢-١-٣}}{=} Ord(Aut(K;P)) \underset{\text{٢-٢-٤}}{=} [K:P] = n$$

($K \cong P^n$ فراغ خطى على P)

ونحتاج فقط للبرهنة على أن قوى هومومورفيزم – فوربينيس σ لـــ K وهى σ^0 ، σ^1 ، ... ، σ^{n-1} مختلفة مثنى مثنى . ولهذا ليكن a عنصراً مولداً للزمرة K^* . لأن $\sigma^i(a) = a^{p^i}$ لجميع i ، يكفى أن نبرهن على أن العناصر a ، a^p ، ... ، $a^{p^{n-1}}$ مختلفة مثنى مثنى . من $a^{p^i} = a^{p^j}$ حيث $i, j \in \{0,...,n-1\}$ ، $j < i$ يكون لدينا $a^{p^j(p^{i-j}-1)} = 1$ ، $0 \leq p^j(p^{i-j}-1) \leq p^j - 1 < p^n - 1$ ، وهذا غير ممكن لأن $Ord(a) = p^n - 1$.

<u>٢-٦-١١ استنتاج</u> :

ليكن $n \in \mathbb{N} \setminus \{0\}$ ، p عدداً أولياً . إذا كان K حقلاً يتكون من p^n من العناصر ، σ هومومورفيزم فوربينيس له ، عندئذ فإن الحقل $Fix(K;[\sigma^i])$ حيث i قاسم لـــ n ، $i \in \mathbb{N} \setminus \{0\}$ يكون حقلاً جزئياً من K .

وعلى وجه الخصوص لكل قاسم i لـــ n يوجد بالضبط حقل جزئى واحد فى K يتكون من p^i من العناصر .

<u>البرهان</u> : من(١-١١-١٢) فى نظرية الزمر، ومن (٢-٦-١٠)السابقة مباشرة فإن الزمر $[\sigma^i]$ ، حيث i قاسم لـــ n ، $i \in \mathbb{N} \setminus \{0\}$ هى الزمر الجزئية الوحيدة من $Aut(K)$.

وهى مختلفة مثنى مثنى ، $Ord([\sigma^i]) = \frac{n}{i}$ ، وبالتالى فإن $[Aut(K):[\sigma^i]] = i$.

والآن من نظرية جالوا الأساسية(٢-٢-٤) فإنه لأى حقل بينى P فى $K \supset \mathbb{Z}/p\mathbb{Z}$ يكون

$$[P : \mathbb{Z}/p\mathbb{Z}] = [Aut(K; \mathbb{Z}/p\mathbb{Z}) : Aut(K;P)]$$

$$= [Aut(K) : Aut(K;P)] \qquad \text{(من ٢-١-٣)}$$

بأخذ $P = Fix(K;[\sigma^i])$ ينتج ان

$$[P : \mathbb{Z}/p\mathbb{Z}] = i$$

ومن (٢-٦-١) ينتج المطلوب مباشرة .

أمثلة متنوعة (٢)

مثال ١ : حدد : أى التقارير الآتية صائب وأيها خاطئ

(١) كثيرة الحدود X^3+5 قابلة للانفصال على $\mathbb{Z}_7$

(٢) كل امتدادات الحقول المنتهية تكون طبيعية

(٣) كل امتداد قابل للانفصال يكون طبيعياً

(٤) كل امتداد طبيعى منته يكون حقل تشقيق لكثيرة حدود

(٥) $\mathbb{Q}(\sqrt{19}) \supset \mathbb{Q}$ امتداد طبيعى وقابل للانفصال

(٦) $\mathbb{Q}(\sqrt{21}) \supset \mathbb{Q}$ امتداد طبيعى وقابل للانفصال

(٧) أى كثيرة حدود قابلة للتحليل لايمكن أن تكون قابلة للانفصال

(٨) إذا كان $D(f)=0$ فإن $f=0$ لكثيرة حدود f على حقل ما .

الحل : التقارير (١) ، (٤) ، (٥) ، (٦) صحيحة . والباقية خاطئة .

مثال ٢ : حدد أى هذه الامتدادات يكون طبيعياً :

(١) $\mathbb{Q}(t) \supset \mathbb{Q}$

(٢) $\mathbb{Q}(\sqrt{-5}) \supset \mathbb{Q}$

(٣) $\mathbb{Q}(\alpha) \supset \mathbb{Q}$ حيث α هو الجذر الحقيقى فى الجذور $\{5^{\frac{1}{7}}\}$

(٤) $\mathbb{Q}(\sqrt{5},\alpha) \supset \mathbb{Q}(\alpha)$ حيث α مثلما فى (٣)

(٥) $\mathbb{R}(\sqrt{-7}) \supset \mathbb{R}$

الحل : الامتدادات (٢) ، (٤) ، (٥) طبيعية .

الامتداد (١) ليس جبريا ، وبالتالى فهو ليس طبيعياً .

بالنسبة إلى التقرير (٣) : كثيرة الحدود X^7-5 لها صفر هو الجذر الحقيقى فى الجذور $\{5^{\frac{1}{7}}\}$ أى لها العامل $X-\alpha$ لكنها لاتتشقق على $\mathbb{Q}(\alpha)$ فى عوامل خطية .

إذن الامتداد ليس طبيعياً .

مثال ٣ : اوجد $Aut(\mathbb{C};\mathbb{R})$

الحل : ليكن $\alpha \in Aut(\mathbb{C};\mathbb{R})$ ، أى أن $\alpha \in Aut(\mathbb{C})$ بحيث يكون :

$$\forall r \in \mathbb{R} : \alpha(r) = r$$

والآن ليكن $\alpha(i) = j$ حيث $i = \sqrt{-1}$. عندئذ فإن :

(لأن $\alpha(r) = r$ لجميع $r \in \mathbb{R}$) $\quad j^2 = \alpha(i)^2 = \alpha(i^2) = \alpha(-1) = -1$

α أوتومورفيزم

ومن ثم فإن $j = i$ أو $j = -i$.

والآن لجميع $x, y \in \mathbb{R}$ لدينا :

(حسب تعريف α) $\quad \alpha(x+iy) = \alpha(x) + \alpha(i)\alpha(y) = x + jy$

والآن لدينا مرشحان :

$$\alpha_1 : \mathbb{C} \to \mathbb{C}, x+iy \mapsto x+iy,$$
$$\alpha_2 : \mathbb{C} \to \mathbb{C}, x+iy \mapsto x-iy$$

واضح أن α_1 هو راسم الوحدة ، ومن ثم فهو ينتمى إلى $Aut(\mathbb{C},\mathbb{R})$

سنثبت أن α_2 كذلك ينتمى إلى $Aut(\mathbb{C};\mathbb{R})$ كالآتى :

$$\begin{aligned}\alpha_2((x+iy)+(u+iv)) &= \alpha_2(x+u+i(y+v)) = x+u-i(y+v)\\ &= x-iy+u-iv\\ &= \alpha_2(x+iy)+\alpha_2(u+iv)\end{aligned}$$

$$\begin{aligned}\alpha_2((x+iy)(u+iv)) &= \alpha_2(xu-yv+i(xv+yu))\\ &= xu-yv-i(xv+yu)\\ &= (x-iy)(u-iv)\\ &= \alpha_2(x+iy)\alpha_2(u+iv)\end{aligned}$$

أى أن α_2 أوتومورفيزم . كذلك فإن :

$$\alpha_2(x+0i) = x-0i = x$$

أى أن $\alpha_2 \in Aut(\mathbb{C};\mathbb{R})$

وواضح أن $\alpha_2^2 = \alpha_1$. ومن ثم فإن $Aut(\mathbb{C};\mathbb{R}) \cong \mathbb{Z}_2$

(زمرة دائرية من الرتبة 2)

مثال ٤ :

لتكن $f := X^4 - 4X^2 - 5 \in \mathbb{Q}[X]$ عين $Gal.(f;\mathbb{Q})$ ، حيث $Gal.(f;\mathbb{Q}) := Aut(K;\mathbb{Q})$ ، K تشقيق f على $\mathbb{Q}$. وعين الحقول الثابتة المناظرة للزمر الجزئية الفعلية من $Gal.(f,\mathbb{Q})$

الحل :

$$f := X^4 - 4X^2 - 5 = (X^2+1)(X^2-5) = 0$$

أى أن أصفار f هى $\alpha = i$ ، $\beta = -i$ ، $\gamma = \sqrt{5}$ ، $\delta = -\sqrt{5}$ ويكون امتداد الحقل المصاحب هو : $K \supset \mathbb{Q}$ حيث $K = \mathbb{Q}(i,\sqrt{5})$. ويكون هناك أربعة عناصر فى $Aut(K;\mathbb{Q})$ هى I ، R ، S ، T ، حيث I هو راسم الوحدة ، $R = (\alpha\beta)$ ، $S = (\gamma\delta)$ ، $T = (\alpha\beta)(\gamma S)$ بالاصطلاح الدائرى . وفى الواقع فإن هذه هى كل عناصر $Aut(K;\mathbb{Q})$ لأن أى عنصر فى $Aut(K;\mathbb{Q})$ يجب أن "يرسل" i إلى $\pm i$ ، $\sqrt{5}$ إلى $\pm\sqrt{5}$. ومن ثم فإن

$$Gal.(f;\mathbb{Q}) := Aut(K;\mathbb{Q}) = \{I, R, S, T\}$$

وتكون الزمر الجزئية الفعلية من $Gal.(f;\mathbb{Q})$ هى :

$$\{I\}, \{I,R\}, \{I,S\}, \{I,T\}$$

وتكون الحقول الثابتة المناظرة هى :

$$K = \mathbb{Q}(i,\sqrt{5}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(i), \mathbb{Q}(i\sqrt{5})$$

ويمكن البرهنة على أن هذه مع $\mathbb{Q}$ هى كل الحقول الجزئية من K .

(لاحظ أنه يوجد تناظر أحادى بين الزمر الجزئية الفعلية من زمرة جالوا ، الحقول الثابتة المناظرة)

<u>مثال ٥</u> : حدد : أى التقارير الآتية صائب وأيها خاطئ :

(١) كل عنصر فى $Aut(K;k)$ هو عنصر فى $Aut(K)$

(٢) كل عنصر فى $Aut(K;K)$ هو راسم الوحدة

(٣) زمرة جالوا $Aut(K;k)$ دائرية

(٤) زمرة جالوا $Aut(\mathbb{C};\mathbb{R})$ إبدالية

(٥) الراسمان $Aut(K;\ )$ ، $Fix(K;\ )$ فى (٢-٢-٤) كل منهما معكوس الآخر

(٦) الراسمان السابقان يحفظان الاحتواءات

(٧) إذا كان $Aut(K;k)=\{1\}$ فإن $K=k$

(٨) إذا كان $K=k$ فإن $Aut(K;k)=\{1\}$

(٩) $Ord(K(X);K)=1$

(١٠) تعريف زمر جالوا أسهل من حسابها !

<u>الحل</u> : التقارير (١) ، (٢) ، (٤) ، (٥) ، (٨) ، (١٠) صحيحة . الباقى خاطئ

<u>مثال ٦</u> : اوجد $Aut(K;k)$ للامتدادات $K\supset k$ الآتية :

(أ) $Aut(\mathbb{Q}(\sqrt{2});\mathbb{Q})$

(ب) $Aut(\mathbb{Q}(\alpha);\mathbb{Q})$ حيث α هو الجذر الحقيقى فى الجذور $\{\sqrt[5]{7})$

(جـ) $Aut(\mathbb{Q}(\sqrt{2},\sqrt{3});\mathbb{Q})$

<u>الحل</u> : (أ)

$$(\varphi(\sqrt{2}))^2 := \varphi(\sqrt{2})\varphi(\sqrt{2}) \quad = \quad \varphi(\sqrt{2}\sqrt{2})=\varphi(2) \quad = \quad 2$$

تعريف الامتداد φ أوتومورفيزم

$$\Rightarrow \varphi(\sqrt{2})=\pm\sqrt{2}$$

أى أنه يوجد φ_1 ، φ_2 بحيث يكون

$$\varphi_1(x)=x \qquad \forall x\in\mathbb{Q},$$

$$\varphi_1(\sqrt{2})=\sqrt{2} \quad , \quad \Rightarrow \varphi_1=1;$$

$$\varphi_2(x)=x \qquad \forall x\in\mathbb{Q},$$

$$\varphi_2(\sqrt{2})=-\sqrt{2}$$

أى أن $Aut(\mathbb{Q}(\sqrt{2});\mathbb{Q})$ تتكون من عنصرين ، أحدهما 1 (راسم الوحدة) . ولاحظ أن

$$(\varphi_2(\sqrt{2}))^2=(-\sqrt{2})^2=2,$$

$$\varphi_2(x)=x \quad \forall x\in\mathbb{Q}$$

أى أن $\varphi_2^2=1$. وبالتالى تكون $Aut(\mathbb{Q}(\sqrt{2});\mathbb{Q})$ دائرية لها الرتبة 2 ، أى هى تشاكل $\mathbb{Z}_2$.

(ب)

$$(\varphi(\sqrt[5]{7}))^5 := \varphi(\sqrt[5]{7})^5=\varphi(7) \quad = \quad 7$$

تعريف الامتداد

(لأن $\mathbb{Q}(\sqrt[5]{7})\subset\mathbb{R}$) $\qquad \Rightarrow\varphi(\sqrt[5]{7})=7^{1/5}$

ولأن $\varphi(x)=x \quad \forall x\in\mathbb{Q}$

إذن $\varphi=1$ (راسم الوحدة)

وتكون الزمرة $Aut((\mathbb{Q},\alpha);\mathbb{Q})=\{1\}$

(جـ)

$$(\varphi(\sqrt{2}))^2 := \varphi(\sqrt{2})\varphi(\sqrt{2})=\varphi(\sqrt{2})^2=\varphi(2) \quad = \quad 2\Rightarrow\varphi(2)=\pm\sqrt{2}$$

تعريف الامتداد

$$(\varphi(\sqrt{3}))^2=\varphi(\sqrt{3})\varphi(\sqrt{3})=\varphi(\sqrt{3})^2=\varphi(3) \quad = \quad 3\Rightarrow\varphi(\sqrt{3})=\pm\sqrt{3}$$

تعريف الامتداد

وبذلك يكون لدينا

$$\varphi_1 = 1$$

$$(\varphi_1(\sqrt{2}) = \sqrt{2}, \varphi_1(\sqrt{3}) = \sqrt{3}, \varphi_1(x) = x \quad \forall x \in \mathbb{Q}),$$

$$\varphi_2 : \varphi_2(\sqrt{2}) = -\sqrt{2}, \varphi_2(\sqrt{3}) = \sqrt{3}, \varphi_2(x) = x \quad \forall x \in \mathbb{Q},$$

$$\varphi_3 : \varphi_3(\sqrt{2}) = \sqrt{2}, \varphi_3(\sqrt{3}) = -\sqrt{3}, \varphi_3(x) = x \quad \forall x \in \mathbb{Q},$$

$$\varphi_4 : \varphi_4(\sqrt{2}) = -\sqrt{2}, \varphi_4(\sqrt{3}) = -\sqrt{3}, \varphi_4(x) = x \quad \forall x \in \mathbb{Q},$$

وكما سبق فإن :

$$\varphi_1^2 = \varphi_2^2 = \varphi_3^2 = \varphi_4^2 = 1$$

وتكون

$$Aut(\mathbb{Q}(\sqrt{2}, \sqrt{3}); \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

<u>ملحوظة</u> :

لاحظ أن $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ أساس للفراغ الخطى $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ على الحقل $\mathbb{Q}$.

<u>مثال ٧</u> : باعتبار مثال ٦ السابق والراسمين ($Aut(K;\ )$ ، $Fix(K;\ )$

فى أى الحالات هما تناظران أحاديان ؟

<u>الحل</u> : فى الحالتين (أ) ، (جـ) الامتدادان امتدادا جالوا (انظر (٢-٢-٥))

أما الحالة (ب) فالامتداد ليس امتداد جالوا (انظر (٢-٢-٣))

فى الحالتين (أ) ، (جـ) الراسمان تناظران أحاديان ، وكل منهما معكوس الآخر حسب نظرية جالوا الأساسية (٢-٢-٤) أما فى الحالة (ب) فالراسمان ليسا كذلك .

<u>مثال ٨</u> : برهن على أن كثيرة الحدود $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ قابلة للانفصال.

<u>البرهان</u> : لدينا

$$f := X^4 + X^3 + X^2 + X + 1 = \frac{X^5 - 1}{X - 1}, X \neq 1$$

وتكون أصفار f هى :

$e^{\frac{2\pi i}{5}}$ ، $e^{\frac{4\pi i}{5}}$ ، $e^{\frac{6\pi i}{5}}$ ، $e^{\frac{8\pi i}{5}}$ فى حقل تشقيق داخل

$\mathbb{C}$ ، وكلها مختلفة ، أى كلها بسيطة . وبالتالى فهى قابلة للانفصال .

مثال ٩ :

ليكن K حقلاً منتهياً ، مكوناً من 11 عنصراً . برهن على أن K^* دائرية .

البرهان : لاحظ أن $K = GF(11)$ والآن قوى $\bar{2}$ مرتبة هى :

$$\bar{2},\bar{4},\bar{8},\bar{5},\overline{10},\bar{9},\bar{7},\bar{3},\bar{6},\bar{1}$$

حيث إنه من الواضح أن مميز الحقل هو 11

أى أن $\bar{2}$ مولد لـــ K^* .

مثال ١٠ : حدد إذا ما كانت التقارير الآتية صائبة أم خاطئة :

(١) يوجد حقل منته يتكون من 124 عنصراً

(٢) يوجد حقل منته ، زمرته الضربية تتألف من 124 عنصراً

(٣) يوجد حقل منته يتألف من 125 عنصراً

(٤) الزمرة الضربية للحقل $GF(19)$ بها عنصر رتبته 3

(٥) كل الحقول ذات 121 عنصراً تكون متشاكلة

(٦) $GF(2401)$ يحتوى على حقل جزئى يتشاكل مع $GF(49)$

(٧) أى مونومورفيزم من حقل منته إلى نفسه هو أوتومورفيزم

(٨) الزمرة الجمعية لحقل منته تكون دائرية

(٩) الزمرة الضربية لأى حقل دائرية

(١٠) أس الزمرة هو أكبر رتبة لعناصرها

(يعرف أس الزمرة بأنه المضاعف المشترك الأصغر لرتب عناصرها)

الحل :

(١) خاطئ لأنه لايوجد عدد أولى p وعدد طبيعى n بحيث يكون $p^n = 124$

(٢) ، (٣) : الحقل هنا يتألف من $125 = 5^3$ عنصراً . إذن التقريران صحيحان

(٤) الزمرة الضربية هنا تتألف من 18 عنصراً ، وهى دائرية . إذن التقرير صحيح

(٥) ، (٦) ، (٧) ك تقارير صحيحة

(٨) ، (٩) ، (١٠) : تقرير خاطئة

__مثال ١١ :__

اعتبر الحقل $GF(25)$ أى $GF(5^2)$:

نعتبر العنصر $2+\sqrt{2}$ ، وتكون قواه المختلفة المتتالية محسوبة فى $\mathbb{Z}_5$ هى :

$2+\sqrt{2}$ ، $1+4\sqrt{2}$ ، $4\sqrt{2}$ ، $3+3\sqrt{2}$ ، $2+4\sqrt{2}$ ،

2 ، $4+2\sqrt{2}$ ، $2+3\sqrt{2}$ ، $3\sqrt{2}$ ، $1+\sqrt{2}$ ، $4+3\sqrt{2}$ ،

4 ، $3+4\sqrt{2}$ ، $4+\sqrt{2}$ ، $\sqrt{2}$ ، $2+2\sqrt{2}$ ، $3+\sqrt{2}$ ،

3 ، $1+3\sqrt{2}$ ، $3+2\sqrt{2}$ ، $2\sqrt{2}$ ، $4+4\sqrt{2}$ ، $1+2\sqrt{2}$ ،

1 .

ومن ثم فإن $2+\sqrt{2}$ يولد الزمرة الضربية لـــ $GF(25)$. عناصر $GF(25)$ كلها أصفار لكثيرة الحدود $X^{25}-X \in (GF(25))[X]$ (انظر (٢-٦-٣) ، (٢-٦-٨))

__مثال ١٢ :__

لأى من قيم n الآتية يوجد حقل يتألف من n من العناصر :

1 ، 2 ، 3 ، 4 ، 5 ، 6 ، 17 ، 24 ، 312 ، 65536 ، 65537 ، 83521 ،
$2^{216091}-1$ ، 103823

__الحل :__

الحقل يتألف من n من العناصر إذا كان $n=p^m$ حيث p عدد أولى ، m عدد صحيح موجب. وهذا ينطبق على :

2 ، 3 ، 4 ، 5 ، 17 ، $65536(=2^{16})$ ، 65537 ، $83521(=17^4)$ ، 103823
$2^{216091}-1$.

مثال ١٣ : اوجد $[GF(729):GF(9)]$ ، $[GF(64):GF(8)]$

الحل :

$$[GF(729):GF(9)]=[GF(3^6):GF(3^2)]$$

$$[GF(3^6):GF(3)] \quad = \quad [GF(3^6):GF(3^2)].[GF(3^2):GF(3)]$$

نظرية الدرجة

$$\Rightarrow \; 6=[GF(3^6):GF(3^2)].2$$

١-٦-٢

$$\Rightarrow [GF(729):GF(9)]=[GF(3^6):GF(3^2)]=3.$$

$$[GF(64):GF(8)]=[GF(2^6):GF(2^3)]$$

$$[GF(2^6):GF(2)]=[GF(2^6):GF(2^3)][GF(2^3):GF(2)]$$

$$\Rightarrow \quad 6=[GF(2^6):GF(2^3)].3$$

$$\Rightarrow [GF(64):GF(8)]=[GF(2^6):GF(2^3)]=2$$

مثال ١٤ : برهن على أنه لكل قاسم m لـــ n يوجد حقل جزئى وحيد من $GF(p^n)$ ويتكون من p^m من العناصر. علاوة على هذا لاتوجد حقول جزئية أخرى من $GF(p^n)$

البرهان : للبرهنة على الوجود نفترض أن m تقسم n . عندئذ ، لأن :

$$p^n-1=(p^m-1)(p^{n-m}+p^{n-2m}+...+p^m+1),$$

فإن p^m-1 تقسم p^n-1 . هذا يستلزم أن $X^{p^m-1}-1$ تقسم $X^{p^n-1}-1$ فى $\mathbb{Z}_p[X]$.

وبالتالى فإن كل صفر لـــ $X(X^{p^m-1}-1)$ هو صفر لـــ $X(X^{p^n-1}-1)$. ومن (٢-٦-٨) فإن مجموعة أصفار $X(X^{p^m-1}-1)$ هى $GF(p^m)$ ، وكذلك فإن مجموعة

أصفار $X(X^{p^n-1}-1)$ فى $GF(p^n)$ هى $GF(p^n)$. ومن ثم فإن $GF(p^m)$ هو حقل جزئى من $GF(p^n)$ ما دامت m تقسم n .

الوحدانية تنتج من ملاحظة أنه إذا كان $GF(p^n)$ له حقلان جزئيان مختلفان من الرتبة p^m فإن كثيرة الحدود $X^{p^m}-X$ يكون لهما أكثر من p^m صفراً فى $GF(p^n)$. هذا بالطبع يناقض (٢-٢-٣) فى نظرية الحلقات

وأخيراً ليكن F حقلاً جزئياً من $GF(p^n)$. عندئذ فإن F يتشاكل مع $GF(p^m)$ لبعض m ، ويكون لدينا :

$$n=[GF(p^n):\ GF(p)]$$

$$=[GF(p^n):GF(p^m)][GF(p^m):GF(p)]$$

$$=[GF(p^n):GF(p^m)]m$$

أى أن m تقسم n .

<u>مثال ١٥</u> : إذا كان F حقلاً مكوناً من 729 عنصراً ، وكان α مولداً لـــ F^* (الزمرة الضربية لـــ F) فاوجد الحقول الجزئية

$GF(729)$ ، $GF(27)$ ، $GF(9)$ ، $GF(3)$

<u>الحل</u> :

$$GF(3)=\{0\}\cup[\alpha^{364}]=\{\bar{0},\bar{1},\bar{2}\}$$

$$GF(9)=\{0\}\cup[\alpha^{91}]$$

$$GF(27)=\{0\}\cup[\alpha^{28}]$$

$$GF(729)=\{0\}\cup[\alpha]$$

لاحظ أن هذه هي كل الحقول الجزئية و ذلك من المثال السابق مباشرة.

مثال ١٦ : وضح بالرسم الاحتواءات التى تربط الحقول الجزئية من $GF(2^{24})$

الحل : الحقول الجزئية الفعلية من $GF(2^{24})$ هى :

$GF(2)$ ، $GF(2^2)$ ، $GF(2^3)$ ، $GF(2^4)$ ، $GF(2^6)$ ، $GF(2^8)$ ، $GF(2^{12})$.

(انظر (٢-٦-١١))

$GF(2^8) \subset GF(2^{24})$

$GF(2^4)$ — $GF(2^{12})$

$\cup \qquad \cup$

$GF(2^6)$

$GF(2^2) \qquad GF(2^3)$

$GF(2)$

مثال ١٧ : اوجد الحقول الجزئية من $GF(16)$

الحل :

$$GF(16) \cong \{aX^3 + bX^2 + cX + d + [X^4 + X + 1] \mid a,b,c,d \in \mathbb{Z}_2\}$$

(تمرين (٤) فى تمارين عامة (٢))

والآن لاحظ أن

$$\overline{X^4 + X + 1} = \bar{0} \Rightarrow \overline{X^4} = \overline{-X - 1}$$

$$= \overline{X+1} \qquad (1)$$

$$\Rightarrow \overline{X^5} = \overline{X^2+X} \qquad (2)$$

$$\Rightarrow \overline{X^{10}} = \overline{(X^2+X)^2} = \overline{X^4+2X^3+X^2}$$

$$= \overline{X+1+0+X^2}$$

$$= \overline{X^2+X+1} \qquad (3)$$

ومن حيث إن الحقل يتكون من 16 عنصراً فإن الحقول الجزئية منه تتكون من عنصرين ، أربعة عناصر ، ستة عشر عنصراً .

واضح أن الحقل الجزئى المكون من عنصرين هو $\{\overline{0},\overline{1}\}$. كذلك الحقل الجزئى المكون من ستة عشر عنصراً هو الحقل نفسه . يتبقى أن نجد الحقل المكون من أربعة عناصر . ونعلم أن العناصر الثلاثة غير الصفرية فيه تكون زمرة جزئية دائرية من الزمرة الضربية الدائرية $(GF(16))^*$. (الزمرة الجزئية من زمرة دائرية تكون دائرية) .

ومن (١-١١-١٢) فى نظرية الزمر فإن $X^3+[X^4+X+1]$ (أو $\overline{X^3}$) ، $X^5+[X^4+X+1]$ (أو $\overline{X^5}$) ، هما المولدان الوحيدان للزمرتين الجزئيتين الفعليتين من $(GF(16))^*$ (لأن 3 ، 5 هما القاسمان الوحيدان "غير التافهين" لـ15) .

$\overline{X^3}$ تنتج زمرة جزئية ذات خمسة عناصر ، من $(GF(16))^*$ ، بينما $\overline{X^5}$ تنتج زمرة جزئية ذات ثلاثة عناصر من $(GF(16))^*$ ، أى تنتج حقلاً جزئياً ذا أربعة عناصر من $GF(16)$ ويكون الحقل الجزئى ذو الأربعة عناصر هو :

$$\{\overline{0},\overline{1},\overline{X^5},\overline{X^{10}}\} = \{\overline{0},\overline{1},\overline{X^2+X},\overline{X^2+X+1}\}$$

التحقيق $\overline{X^5} \neq \overline{1}$ لأن $\overline{X^5} = \overline{1}$ يقتضى أن $\overline{1} = \overline{X^{10}}$.

ومن (3) لدينا $\overline{X^{10}} = \overline{X^2+X+1}$ ، ومن ثم فإن $\overline{X^2+X+1} = \bar{1}$ ، أى أن $\overline{X^2+X} = \bar{0}$ ، ومن (2) يكون $\bar{1} = \bar{0}$: تناقض .

$\overline{X^{10}} \neq \bar{1}$ وإلا ، فلدينا مما سبق أن $\overline{X^{10}} = \overline{X^2+X+1}$ وبهذا يكون $\overline{X^2+X} = \bar{0}$ ومن (2) يكون $\overline{X^5} = \bar{0}$ أى أن $\overline{X} = \bar{0}$ أى أن $X \in [X^4+X+1]$: تناقض .

<u>مثال ١٨</u> : برهن على أن $\overline{X}$ مولد للزمرة الدائرية $\left(\mathbb{Z}_3[X] \big/ [X^3+2X+1]\right)^*$

<u>البرهان</u> :

$$F := \mathbb{Z}_3[X] \big/ [X^3+2X+1] = \{aX^2+bX+c+[X^3+2X+1] \mid a,b,c \in \mathbb{Z}_3\}$$

ومن ثم فإن عدد عناصر F هو 27 ، ويكون عدد عناصر F^* هو 26 .

وسنثبت أن $\overline{X^2} \neq \bar{1}$ ، $\overline{X^{13}} \neq \bar{1}$. ومن حيث إن 2 ، 13 هما القاسمان الوحيدان غير التافهين لــ 26 ، فإن $\overline{X}$ تكون مولدًا لــ F^* .

$\overline{X^2} = \bar{1}$ يقتضى أن $\overline{X^3} = \overline{X}$. لدينا $\overline{X^3+2X+1} = \bar{0}$. ومن ثم فإن : $\overline{3X+1} = \bar{0}$. وبالتالى فإن $\bar{1} = \bar{0}$: تناقض ($\bar{3} = \bar{0}$ فى $\mathbb{Z}_3$) .

والآن $\overline{X^3+2X+1} = \bar{0}$ يقتضى أن $\overline{X^3} = \overline{X+2}$. ومن ثم فإن :

$$\overline{X^{12}} = \overline{(X+2)^4} = \overline{X^4+4X^3.2+6X^2.4+4X.8+16}$$

$$= \overline{X^4+2X^3+2X+1}$$

$$= \overline{X^4+X^3} \qquad (\text{لأن } \overline{X^3+2X+1} = \bar{0})$$

$$= \overline{X^3(X+1)}$$

$$= \overline{(X+2)(X+1)} = \overline{X^2+3X+2} = \overline{X^2+2}$$

ومن ثم فإن :

$$\overline{X^{13}} = \overline{X^3 + 2X} = \overline{-1} = \overline{2} \neq \overline{1}$$

نهاية البرهان .

مثال ١٩ : لتكن f كثيرة حدود من الدرجة الثالثة غير القابلة للتحليل فى $\mathbb{Z}_2[X]$.
برهن على أن حقل تشقيق f على $\mathbb{Z}_2$ يتكون من 8 عناصر أو 64 عنصراً .

البرهان : إذا كان a صفراً لـــ f . فى امتداد ما فيكون $f = (X-a)\,g$. عندئذ فإن $[\mathbb{Z}_2(a):\mathbb{Z}_2] = 3$. إذا كانت f تتشقق على $\mathbb{Z}_2(a)$ نكون قد انتهينا ويكون عدد عناصر $\mathbb{Z}_2(a)$ هو 2^3 أى 8 . (انظر (٢-٦-١)) .

إذا لم يكن الأمر كذلك ، فليكن b صفراً لـــ g فى امتداد ما لـــ $\mathbb{Z}_2(a)$.

عندئذ فإن $[\mathbb{Z}_2(a,b):\mathbb{Z}_2(a)] = 2$ (g من الدرجة الثانية !) وبهذا يكون

$$[\mathbb{Z}_2(a,b):\mathbb{Z}_2] = [\mathbb{Z}_2(a,b):\mathbb{Z}_2(a)][\mathbb{Z}_2(a):\mathbb{Z}_2] = 2.3 = 6$$

وبالتالى يكون عدد عناصر $\mathbb{Z}_2(a,b)$ هو 2^6 أى 64

مثال ٢٠ : برهن على أن أكبر درجة لعامل غير قابل للتبسيط من عوامل $X^8 - X$ على $\mathbb{Z}_2$ هى 3.

البرهان : لاحظ أولاً أن $GF(8)$ هو حقل تشقيق $X^8 - X$ (انظر (٢-٦-٨)).
كذلك فإن :

$[GF(8):GF(2)(=\mathbb{Z}_2)] = 3$ وينتج المطلوب (لماذا ؟)

مثال ٢١ : برهن على أن X ليس مولداً للزمرة الدائرية $\left(\mathbb{Z}_3[X]\big/[X^3+2X+2]\right)^*$

الحل :

$$F := \mathbb{Z}_3[X]\big/[X^3+2X+2] = \{aX^2 + bX + c + [X^3+2X+2] \mid a,b,c \in \mathbb{Z}_3\}$$

ويكون عدد عناصر $F = 3^3$ أى ٢٧ . ومن ثم فإن عدد عناصر F^* هو 26 .

والآن : $X^3+\bar{2}X+\bar{2}=\bar{0}$ يقتضى أن $X^3=X+\bar{1}$ (الحساب فى $\mathbb{Z}_3[X]$)

وهذا يقتضى أن : (1) $X^4=X^2+X$. كذلك يكون لدينا :

$$X^{12}=(X+\bar{1})^4=X^4+\bar{4}X^3+\bar{6}X^2+\bar{4}X+\bar{1}$$

$$=X^4+X^3+X+\bar{1}$$

$$\underset{(1)}{=}X^3+X^2+\bar{2}X+\bar{1}$$

$$=X+\bar{1}+X^2+\bar{2}X+\bar{1} \qquad (\text{لأن } X^3=X+\bar{1})$$

$$=X^2+\bar{2}$$

$$\Rightarrow X^{13}=X^3+\bar{2}X=\bar{1} \qquad (\text{لأن } X^3+\bar{2}X+\bar{2}=\bar{0})$$

أى أن X تولد زمرة جزئية من F^* رتبتها 13 ، وبهذا لاتكون مولدة لـــ F^* .

<u>مثال ٢٢</u> :

ليكن E حقل تشقيق لـــ $f:=X^{p^n}-X$ على $\mathbb{Z}_p$. برهن على أن مجموعة أصفار f فى E مغلقة تحت الجمع والطرح والضرب والقسمة .

<u>البرهان</u> : ليكن لدينا $x^{p^n}=x$ ، $y^{p^n}=y$ فى E . ينتج أن

$$x^{p^n}+y^{p^n}=x+y \qquad (*)$$

ومن مثال ٨ فى (١-١-١٠) : $(*')$ $(x+y)^{p^n}=x^{p^n}+y^{p^n}$ ، وبالتالى فإن :

$$(x+y)^{p^n}=x+y$$

أى أنه إذا كان x ، y جذرين للمعادلة $X^{p^n}=X$

فإن $x+y$ جذر للمعادلة $X^{p^n}-X=0$

بعبارة أخرى إذا كان x ، y صفرين للدالة $X^{p^n}-X$ فإن $x+y$ صفر لها .

وبوضع $-y$ بدلاً من y فى (*) ، (*') (سواء كانت $p=2$ أو p عدد أولى فردى) فإنه ينتج أن

$$(x-y)^{p^n} = x-y$$

أى أن $x-y$ أيضاً صفر للدالة $X^{p^n}-X$

كذلك فإنه ينتج من أن x ، y صفرين للدالة $X^{p^n}-X$ أن

$$(\frac{x}{y})^{p^n} = \frac{x}{y}, y \neq 0$$

أى أنه $\frac{x}{y}$ صفر لنفس الدالة .

كذلك فإن :

$$(xy)^{p^n} \;=\; x^{p^n} y^{p^n} = xy$$

E إبدالى

أى أن xy صفر لنفس الدالة .

<u>مثال ٢٣</u> : حدد إذا ما كانت التقارير الآتية صائبة أم خاطئة :

(١) أصفار $X^{28}-1 \in \mathbb{Q}[X]$ فى $\mathbb{C}$ تكون زمرة دائرية مع عملية الضرب

(٢) يوجد حقل منته يتألف من 60 عنصراً

(٣) يوجد حقل منته يتألف من 36 عنصراً

(٤) العدد المركب i هو جذر رابع بدائى للوحدة

(تعريف : يقال لعنصر α فى حقل إنه جذر نونى بدائى للوحدة primitive n^th root of unity) إذا كان $\alpha^n=1$ ، $\alpha^m \neq 1$ لـ $0<m<n$)

(٥) توجد كثيرة حدود غير قابلة للتبسيط (للتحليل) من درجة 58 فى $\mathbb{Z}_2[X]$

(٦) العناصر غير الصفرية فى $\mathbb{Q}$ تكون زمرة دائرية $\mathbb{Q}^*$ مع عملية الضرب

(٧) إذا كان F حقلاً منتهياً ، فإن كل أيزومورفيزم (تشاكل) يرسم F إلى إغلاق جبرى $\overline{F}$ لـــ F يكون أوتومورفيزما لـــ F .

الحل : (١) ، (٤) ، (٥) ، (٧) صحيحة . باقى التقارير خاطئ .

مثال ٢٤ :

(أ) اوجد عدد الجذور البدائية الثمانية (primitive 8 th roots) للوحدة فى $GF(9)$

(ب) اوجد عدد الجذور البدائية الثمانى عشرية (primitive 18 th roots) للوحدة فى $GF(19)$

(جـــ) اوجد عدد الجذور البدائية الخمس عشرية (primitive 15 th roots) للوحدة فى $GF(31)$

(د) اوجد عدد الجذور البدائية العشرية (primitive 10 th roots) للوحدة فى $GF(23)$

الحل :

(أ) عدد العناصر فى $(GF(9))^*$ هو 8 . المطلوب إذن حسب التعريف الوارد فى المثال السابق مباشرة هو إيجاد عدد مولدات $(GF(9))^*$. (لاحظ أن $(GF(9))^*$ دائرية حسب (٢-٦-٣). ومن (١-١١-١١) فى نظرية الزمر يكون عدد المولدات هو عدد "r" بحيث يكون القاسم المشترك الأعظم لـــ n ، r هو الواحد . وبالتالى يكون العدد المطلوب هو 4 .

(ب) عدد العناصر فى $(GF(19))^*$ هو 18 . وتماماً كما فى (أ) يكون العدد المطلوب هو عدد "r" بحيث يكون القاسم المشترك الأعظم لـــ n ، r هو "1" . وبالتالى يكون العدد المطلوب هو 6 .

(جـــ) هنا يتطلب الموقف الرجوع إلى التمرين (٨٤) فى تمارين عامة على الباب الاول فى نظرية الزمر . المطلوب هو تعيين عدد العناصر a^x الموضحة كالآتى :-

ليكن a مولداً لـــ $(GF(31))^*$ الذى يتألف من 30 عنصراً . سيولد a^x زمرة جزئية من $(GF(31))^*$ عدد عناصرها 15 إذا كان : d القاسم المشترك الأعظم لـــ x ، 30 وكان $\frac{n}{d}=15$، أى أن $d=2$. وبالتالى يكون $x=2, 4, 8, 14, 16, 22, 26, 28$

والعدد المطلوب يساوى 8 .

(د) نتخذ نفس الأسلوب المتبع فى (جـــ) . ولكن نلاحظ هنا أنه لايوجد d بحيث يكون $10=\frac{22}{d}=\frac{n}{d}$. وبالتالى لايوجد a^x بحيث يكون مولداً لزمر جزئية من $(GF(23))^*$ عدد عناصرها 10 .

<u>**مثال ٢٥**</u> : ليكن p عدداً أولياً فردياً .

(أ) برهن على أنه لـــ $a \in \mathbb{Z}$ ، حيث $a \not\equiv 0(\bmod p)$ ، فإن المعادلة $x^2 \equiv a(\bmod p)$ لها حل فى $\mathbb{Z}$ إذا كان وفقط إذا كان $a^{\frac{p-1}{2}} \equiv 1(\bmod p)$.

(ب) استخدم الجزء (أ) لمعرفة إذا ما كانت كثيرة الحدود X^2-6 غير قابلة للتحليل فى $\mathbb{Z}_{17}[X]$

<u>**الحل**</u> : (أ)

$$x^2 \equiv a(\bmod p) \Rightarrow \exists n \in \mathbb{Z} : a = x^2 - np$$

$$\Rightarrow a^{\frac{p-1}{2}} = (x^2-np)^{\frac{p-1}{2}}$$

$$= x^{p-1} + \frac{p-1}{2}(x^2)^{\frac{p-1}{2}-1}.(-np) + \ldots$$

$$+ \binom{\frac{p-1}{2}}{r}(x^2)^{\frac{p-1}{2}-r}.(-np)^r + \ldots + (-np)^{\frac{p-1}{2}}$$

$$\equiv x^{p-1}(\bmod p)$$

إذا كانت $x \in \mathbb{Z}$ فإن $x^{p-1} \in \mathbb{Z}$ ويكون $x^{p-1} \equiv 1(\mod p)$ لأننا بالحساب فى $\mathbb{Z}_p$ لدينا لجميع $x^{p-1} \equiv 1(\mod p) : x \in \mathbb{Z}_p^*$ (رتبة العنصر فى الزمرة تقسم رتبة الزمرة . هنا رتبة الزمرة الدائرية (الضربية) $\mathbb{Z}_p^*$ هى p- 1)

(لاحظ أن $x \neq 0$ وإلا كان $a \equiv 0(\mod p)$)

وبالعكس إذا كان $a^{\frac{p-1}{2}} \equiv 1(\mod p)$ فإن $x^{p-1} \equiv 1(\mod p)$ وينتج أن $x \in \mathbb{Z}$.

(ب) $X^2 - 6$ غير قابلة للتحليل فى $\mathbb{Z}_{17}[X]$ أى أن المعادلة $x^2 \equiv 6(\mod 17)$ ليس لها حل فى $\mathbb{Z}$: من (أ) $x^2 \equiv 6(\mod 17)$ لها حل فى $\mathbb{Z}$ إذا كان وفقط إذا كان $6^{\frac{17-1}{2}} \equiv 1(\mod 17)$ ، أى إذا كان وفقط إذا كان

$$6^8 - 1 = 17k , k \in \mathbb{Z}$$

والآن :

$$\begin{aligned} 6^8 - 1 &= (6^4 + 1)(6^2 + 1)(6^2 - 1) \\ &= (1297)(37)(35) \end{aligned}$$

وواضح أنه لا يوجد $K \in \mathbb{Z}$ بحيث يكون

$$(1297)(37)(35) = 17\,K$$

إذن $X^2 - 6$ غير قابلة للتحليل فى $\mathbb{Z}_{17}[X]$.

<u>**مثال ٢٦**</u> : ليكن F حقلاً منتهيا له المميز p . عندئذ فإن كثيرة الحدود $X^{p^n} - X$ لها p^n أصفار مختلفة فى حقل تشقيقها $K \subset \overline{F}$ على F .

<u>**البرهان**</u> : ليكن F حقلاً منتهيا له المميز p ، وليكن K فى $\overline{F}$ حقل تشقيق كثيرة الحدود $X^{p^n} - X$ على F . سنبرهن على أن $X^{p^n} - X$ لها p^n من الأصفار المختلفة فى K .

واضح أن 0 صفر لكثيرة الحدود $X^{p^n}-X$ ، وتكراره 1 أى هو صفر بسيط .

والآن ليكن $\alpha \neq 0$ صفراً لـ $X^{p^n}-X$ وبالتالى هو صفر لـ $f := X^{p^n-1}-1$. عندئذ فإن $X-\alpha$ هو عامل من عوامل f فى $K[X]$ ، وبالقسمة المطولة نحصل على :

$$\frac{f}{X-\alpha} = g = X^{p^n-2} + \alpha X^{p^n-3} + \alpha^2 X^{p^n-4} + \ldots + \alpha^{p^n-3} X + \alpha^{p^n-2}$$

وبهذا تتكون g من p^n-1 من الحدود ، وفى $g(\alpha)$ يكون كل حد هو :

$$\alpha^{p^n-2} = \frac{\alpha^{p^n-1}}{\alpha} = \frac{1}{\alpha}$$

(لأن $f(\alpha) = 0 = \alpha^{p^n-1}-1$)

وهكذا فإن :

$$g(\alpha) = (p^n-1).\frac{1}{\alpha} = -\frac{1}{\alpha}$$

لأننا فى حقل مميزه p . وبالتالى فإن $g(\alpha) \neq 0$ ، α صفر بسيط لـ f أى له التكرار 1 .

<u>تعريف</u> : ليكن E امتداداً جبرياً لحقل F . يقال لعنصرين $\alpha, \beta \in E$ إنهما **<u>مترافقان</u>** على F (conjugate over F) إذا كان α ، β صفرين لنفس كثيرة الحدود غير القابلة للتبسيط على F.

<u>مثال ٢٧</u> : هل يتطابق مفهوم الترافق المعرف أعلاه مع فكرة الأعداد المركبة المترافقة التقليدية ؟

<u>الحل</u> : نعم ، إذا كنا نعنى بعددين مركبين مترافقين أنهما مترافقان على $\mathbb{R}$. فإذا كان $a,b \in \mathbb{R}$ ،

فالعددان المركبان $b \neq 0$ $a+ib$ ، $a-ib$ هما صفران لكثيرة الحدود $X^2-2aX+a^2+b^2$ ، التى هى غير قابلة للتحليل (للتبسيط) فى $\mathbb{R}[X]$. (تحقق من ذلك).

<u>مثال ٢٨</u> : اعتبر امتداد الحقل $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$. أصفار كثيرة الحدود (المطبعة غير القابلة للتبسيط على $\mathbb{Q}$) X^2-2 هما $\sqrt{2}$ ، $-\sqrt{2}$ ، وهكذا فإن $\sqrt{2}$ ، $-\sqrt{2}$ مترافقان على $\mathbb{Q}$.

لاحظ أن الراسم

$$\psi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$
$$a+b\sqrt{2} \mapsto a-b\sqrt{2}$$

هو أيزومورفيزم من $\mathbb{Q}(\sqrt{2})$ على نفسه ، أى هو أوتومورفيزم على $\mathbb{Q}(\sqrt{2})$.

<u>مثال ٢٩</u>: اوجد الحقل الثابت فى $\mathbb{Q}(\sqrt{2})$ بالأوتومورفيزم المعطى فى مثال ٢٨ السابق.

<u>الحل</u> : لجميع $a,b \in \mathbb{Q}$ لدينا :

$$\psi(a+b\sqrt{2}) = a-b\sqrt{2}$$

وبالتالى يكون لدينا $a+b\sqrt{2} = a-b\sqrt{2}$ ، ومن ثم هذا يحدث إذا كان وفقط إذا كان $b=0$. أى أن الحقل الثابت هو $\mathbb{Q}$.

<u>مثال ٣٠</u> : حدد أى التقارير الآتية صحيح ، وأيها خاطئ :

(أ) لجميع $\alpha, \beta \in E$ يوجد دائماً أوتومورفيزم لــ E يرسم α على β .

(ب) لــ α, β الجبريين على حقل F ، يوجد دائماً أيزومورفيزم من $F(\alpha)$ على $F(\beta)$.

(جـ) لــ α , β الجبريين المترافقين على حقل F ، يوجد دائماً أيزومورفيزم من $F(\alpha)$ على $F(\beta)$.

(د) كل أوتومورفيزم لكل حقل يترك كل عنصر فى الحقل الجزئى الأولى من E ثابتاً .

(هـ) كل أوتومورفيزم لكل حقل E يترك عدداً لا نهائياً من عناصر E ثابتة .

(و) كل أوتومورفيزم لكل حقل E يترك على الأقل عنصرين من عناصر E ثابتين .

(ز) كل أوتومورفيزم لكل حقل E مميزه صفر يترك عدداً لا نهائياً من عناصر E ثابتة .

(ح) كل أوتومورفيزمات الحقل E تكون زمرة مع عملية تركيب الرواسم .

(ط) مجموعة عناصر حقل E المتروكة ثابتة بأوتومورفيزم ما لـــ E تكون حقلاً جزئياً من E.

(ى) للحقول $F \subset E \subset K$ يكون $Aut(K;E) \subset Aut(K;F)$

الحل : (أ) ، (ب) ، (هـــ) خاطئة . باقى التقارير صحيحة .

<u>مثال ٣١</u> : اوجد جميع الأعداد المترافقة مع الأعداد الآتية على الحقول المعطاة :

(أ) $\sqrt{2}$ على $\mathbb{Q}$ (ب) $\sqrt{2}$ على $\mathbb{R}$

(جـــ) $3+\sqrt{2}$ على $\mathbb{Q}$ (د) $\sqrt{2}-\sqrt{3}$ على $\mathbb{Q}$

(هـــ) $\sqrt{2}+i$ على $\mathbb{Q}$ (و) $\sqrt{2}+i$ على $\mathbb{R}$

(ز) $\sqrt{1+\sqrt{2}}$ على $\mathbb{Q}$ (ح) $\sqrt{1+\sqrt{2}}$ على $\mathbb{Q}(\sqrt{2})$

<u>الحل</u> : (أ) باستخدام تمرين (٢١) فى تمارين عامة (٢) يكون $\sqrt{2}$ مترافقا مع نفسه ومع $-\sqrt{2}$ على $\mathbb{Q}$. كذلك يمكن أن نستخدم الطريقة الآتية بإيجاد كثيرة الحدود الصغرى لـــ $\sqrt{2}$، واستنتاج أى العناصر تكون هى كثيرة الحدود الصغرى منها :

$$X=\sqrt{2} \Rightarrow X^{2}=2 \Rightarrow X^{2}-2=0$$

وواضح أن كثيرة الحدود هذه هى كثيرة الحدود الصغرى كذلك للعنصر $-\sqrt{2}$ على $\mathbb{Q}$.

(ب) $X-\sqrt{2}$ هى كثيرة الحدود الصغرى لـــ $\sqrt{2}$ على $\mathbb{R}$. فالعنصر $\sqrt{2}$ يترافق مع نفسه فقط على $\mathbb{R}$.

(جـــ) كذلك باستخدام تمرين (٢١) السابق ذكره يكون $3+\sqrt{2}$ مترافقا مع نفسه ومع $3-\sqrt{2}$ على $\mathbb{Q}$.

ويمكن استخدام كثيرة الصغرى لأداء المطلوب ، كما جاء في (أ) كالآتي :

$$X=3+\sqrt{2}\Rightarrow X-3=\sqrt{2}\Rightarrow X^{2}-6X+7=0$$

$$\Rightarrow X=\frac{6\pm\sqrt{36-28}}{2}=3\pm\sqrt{2}$$

أي أن $3+\sqrt{2}$ يترافق مع نفسه ومع $3-\sqrt{2}$ على $\mathbb{Q}$.

سنستخدم تمرين (٢١) المشار إليه لإيجاد باقي الأعداد المترافقة :

(د) $\sqrt{2}-\sqrt{3}$ يترافق مع نفسه ومع $\sqrt{2}+\sqrt{3}$ ومع $-\sqrt{2}-\sqrt{3}$ ومع $-\sqrt{2}+\sqrt{3}$ على $\mathbb{Q}$.

(هـ) $\sqrt{2}+i$ يترافق مع نفسه ومع $-\sqrt{2}+i$ ، $\sqrt{2}-i$ ، $-\sqrt{2}-i$ على $\mathbb{Q}$.

(و) $\sqrt{2}+i$ يترافق مع نفسه ومع $\sqrt{2}-i$ على $\mathbb{R}$.

(ز) $\sqrt{1+\sqrt{2}}$ يترافق مع نفسه ومع $\sqrt{1-\sqrt{2}}$، $-\sqrt{1+\sqrt{2}}$ ، $-\sqrt{1-\sqrt{2}}$ على $\mathbb{Q}$.

(ح) $\sqrt{1+\sqrt{2}}$ يترافق مع نفسه ومع $-\sqrt{1+\sqrt{2}}$ على $\mathbb{Q}(\sqrt{2})$.

<u>ملحوظة</u> : لاحظ أن علاقة الترافق علاقة تكافؤ فهي انعكاسية ومتماثلة وانتقالية .

<u>مثال ٣٢</u> : اعتبر الحقل $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ ، واعتبر الأيزومورفيزمات الآتية ، كما جاءت في تمرين (٢١) المشار إليه :

$$\psi_{\sqrt{2},-\sqrt{2}}:(\mathbb{Q}(\sqrt{3},\sqrt{5}))(\sqrt{2})\rightarrow(\mathbb{Q}(\sqrt{3},\sqrt{5}))(-\sqrt{2})$$

$$\psi_{\sqrt{3},-\sqrt{3}}:(\mathbb{Q}(\sqrt{2},\sqrt{5}))(\sqrt{3})\rightarrow(\mathbb{Q}(\sqrt{2},\sqrt{5}))(-\sqrt{3})$$

$$\psi_{\sqrt{5},-\sqrt{5}}:(\mathbb{Q}(\sqrt{2},\sqrt{3}))(\sqrt{5})\rightarrow(\mathbb{Q}(\sqrt{2},\sqrt{3}))(-\sqrt{5})$$

وللاختصار : ليكن $r_2:=\psi_{\sqrt{2},-\sqrt{2}}$ ، $r_3:=\psi_{\sqrt{3},-\sqrt{3}}$ ، $r_5:=\psi_{\sqrt{5},-\sqrt{5}}$

احسب :

(أ) $r_2(\sqrt{3})$ (ب) $r_2(\sqrt{2}+\sqrt{5})$

(جـ) $(r_2 o r_3)(\sqrt{2}+3\sqrt{5})$ (د) $(r_3 o r_5)(\frac{\sqrt{2}-3\sqrt{5}}{2\sqrt{3}-\sqrt{2}})$

(هـ) $(r_2 o r_3 o r_5^2)(\sqrt{2}+\sqrt{45})$ (و) $r_3(r_5(\sqrt{2}-\sqrt{3})+(r_5 o r_2)(\sqrt{30}))$

<u>الحل</u> :

(أ) $r_2(\sqrt{3})=\sqrt{3}$

(ب) $r_2(\sqrt{2}+\sqrt{5})=-\sqrt{2}+\sqrt{5}$

(جـ)
$$(r_2 o r_3)(\sqrt{2}+3\sqrt{5})=r_2(r_3(\sqrt{2}+3\sqrt{5}))$$
$$=r_2(\sqrt{2}+3\sqrt{5})=-\sqrt{2}+3\sqrt{5}$$

(د)

$$(r_3 o r_5)(\frac{\sqrt{2}-3\sqrt{5}}{2\sqrt{3}-\sqrt{2}})=r_3(r_5(\frac{\sqrt{2}-3\sqrt{5}}{2\sqrt{3}-\sqrt{2}}))=r_3(\frac{\sqrt{2}+3\sqrt{5}}{2\sqrt{3}-\sqrt{2}})$$
$$=\frac{\sqrt{2}+3\sqrt{5}}{-2\sqrt{3}-\sqrt{2}}=-\frac{\sqrt{2}+3\sqrt{5}}{2\sqrt{3}+\sqrt{2}}$$

(هـ)

$$(r_2 o r_3 o r_5^2)(\sqrt{2}+\sqrt{45})=(r_2 o r_3 o 1)(\sqrt{2}+\sqrt{45})$$
$$=(r_2 o r_3)(1(\sqrt{2}+3\sqrt{5}))=(r_2 o r_3)(\sqrt{2}+3\sqrt{5})$$
$$=r_2(r_3(\sqrt{2}+3\sqrt{5}))=r_2(\sqrt{2}+3\sqrt{5})$$
$$=-\sqrt{2}+3\sqrt{5}=-\sqrt{2}+\sqrt{45}$$

(و)

$$r_3(r_5(\sqrt{2}-\sqrt{3})+(r_5 o r_2)(\sqrt{30}))=$$
$$=r_3(\sqrt{2}-\sqrt{3}+r_5(r_2(\sqrt{2}\sqrt{3}\sqrt{5})))$$

$$= r_3(\sqrt{2} - \sqrt{3} + r_5(-\sqrt{2}\sqrt{3}\sqrt{5})) = r_3(\sqrt{2} - \sqrt{3} + \sqrt{2}\sqrt{3}\sqrt{5})$$

$$= \sqrt{2} + \sqrt{3} + \sqrt{2}(-\sqrt{3})\sqrt{5} = \sqrt{2} + \sqrt{3} - \sqrt{30}$$

مثال ٣٣ :

فى المثال (٢-١-٥) كان لدينا الحقل $K := \mathbb{Q}(\sqrt{2},\sqrt{3})$ والأوتومورفيزمات 1_K ، φ_1 ، φ_2 ، φ_3 . حيث $\varphi_1(\sqrt{3}) = -\sqrt{3}$ ، $\varphi_2(\sqrt{2})=-\sqrt{2}$ ، $\varphi_3(\sqrt{2}) = -\sqrt{2}$ ، $\varphi_3(\sqrt{3}) = -\sqrt{3}$ ، $\varphi_1(x) = x$ لجميع $x \in \mathbb{Q}(\sqrt{2})$ ، $\varphi_2(x) = x$ لجميع $x \in \mathbb{Q}(\sqrt{3})$ ، $\varphi_3(x) = x$ لجميع $x \in \mathbb{Q}$

المطلوب حساب الحقول الجزئية الثابتة فى K تحت تأثير :

(أ) $\{\varphi_2, \varphi_3\}$ (ب) $\{\varphi_3\}$ (جـ) $\{\varphi_1, \varphi_3\}$

الحل: المجموعة $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ أساس لـ $\mathbb{Q}(\sqrt{2},\sqrt{3})$ (فراغ خطى) على $\mathbb{Q}$ وبالتالى فإن أى عنصر فى $\mathbb{Q}(\sqrt{2},\sqrt{3})$ يمكن أن يكتب على الصورة : $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ حيث $a,b,c,d \in \mathbb{Q}$.

(أ) العنصر $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ تحت تأثير $\{\varphi_2, \varphi_3\}$ يصبح $a-b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$.

لإيجاد الحقل الجزئى الثابت يجب أن يتحقق :

$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=a-b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$. ومن حيث إن $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ أساس لـ $\mathbb{Q}(\sqrt{2},\sqrt{3})$ على $\mathbb{Q}$ فيكون لدينا :

$$b\sqrt{2} = -b\sqrt{2}, c\sqrt{3} = -c\sqrt{3}, d\sqrt{6} = -d\sqrt{6} \Rightarrow b = c = d = 0$$

ويكون الحقل الثابت هو $\{a \mid a \in \mathbb{Q}\} = \mathbb{Q}$

(ب)

$$\varphi_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

وبالتالى يجب أن يكون

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$$
$$\Rightarrow b=c=0$$

ويكون الحقل الثابت هو $\{a+d\sqrt{6}\mid a,d\in\mathbb{Q}\}=\mathbb{Q}(\sqrt{6})$

(جـ) العنصر $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ تحت تأثير $\{\varphi_1,\varphi_3\}$ يصبح :

$$a-b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$

ويكون مثلما فى (أ) : $b=c=d=0$

ويصبح الحقل الثابت هو $\mathbb{Q}$

مثال ٣٤ : اوجد الحقل الجزئى فى $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ تحت تأثير الأوتومورفيزمات أو مجموعات الأوتومورفيزمات الآتية المعرفة كما فى مثال ٣٢ السابق :

(أ) r_3 (ب) r_3^2 (جـ) $\{r_2,r_3\}$

(د) $r_5 o r_2$ (هـ) $r_5 o r_3 o r_2$ (و) $\{r_2,r_3,r_5\}$

الحل : الفراغ الخطى $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ له الأساس

$$\{1,\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{6},\sqrt{10},\sqrt{15},\sqrt{30}\}$$

على الحقل $\mathbb{Q}$.وبالتالى فإن أى عنصر فى $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ يمكن أن يكتب على الصورة

$$x:=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{5}+e\sqrt{6}+f\sqrt{10}+g\sqrt{15}+h\sqrt{30}$$

حيث $a,b,c,d,e,f,g,h\in\mathbb{Q}$

(أ)

$$r_3(x)=a+b\sqrt{2}-c\sqrt{3}+d\sqrt{5}-e\sqrt{6}+f\sqrt{10}-g\sqrt{15}-h\sqrt{30}$$
$$=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{5}+e\sqrt{6}+f\sqrt{10}+g\sqrt{15}+h\sqrt{30}$$

وهذا يتحقق إذا كان وفقط إذا كان : $c=e=g=h=0$

أى أن الحقل الجزئى الثابت تحت تأثير r_3 يكون هو :

$$\{a+b\sqrt{2}+d\sqrt{5}+f\sqrt{10} \mid a,b,c,d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2},\sqrt{5})$$

(ب) r_3^2 هو راسم الوحدة ، وبالتالى يكون الحقل الجزئى الثابت تحت تأثير r_3^2 هو الحقل نفسه $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$

(جـ) العنصر x تحت تأثير $\{r_2,r_3\}$ يصبح :

$$a-b\sqrt{2}-c\sqrt{3}+d\sqrt{5}-e\sqrt{6}-f\sqrt{10}-g\sqrt{15}-h\sqrt{30}$$

وبالتالى فلإيجاد الحقل الجزئى الثابت تحت تأثير $\{r_2,r_3\}$ يجب أن يكون

$$b=c=e=f=g=h=0$$

ويكون الحقل الجزئى الثابت هنا هو $\{a+d\sqrt{5} \mid a,d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{5})$

(د)

$$\begin{aligned}(r_5 o r_2)(x) &= r_5(r_2(x)) \\ &= r_5(a-b\sqrt{2}+c\sqrt{3}+d\sqrt{5}-e\sqrt{6}-f\sqrt{10}+g\sqrt{15}-h\sqrt{30}) \\ &= a-b\sqrt{2}+c\sqrt{3}-d\sqrt{5}-e\sqrt{6}+f\sqrt{10}-g\sqrt{15}+h\sqrt{30} \\ &= a+b\sqrt{2}+c\sqrt{3}+d\sqrt{5}+e\sqrt{6}+f\sqrt{10}+g\sqrt{15}+h\sqrt{30}\end{aligned}$$

وهذا يحدث إذا كان وفقط إذا كان $b=d=e=g=0$

أى أن الحقل الجزئى الثابت هنا هو :

$$\{a+c\sqrt{3}+f\sqrt{10}+h\sqrt{30} \mid a,c,f,h\in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3},\sqrt{10},\sqrt{30}) = \mathbb{Q}(\sqrt{3},\sqrt{10})$$

(هـ)

$$\begin{aligned}(r_5 o r_3 o r_2)(x) &= r_5(r_3(r_2(x))) \\ &= r_5(r_3(a-b\sqrt{2}+c\sqrt{3}+d\sqrt{5}-e\sqrt{6}-f\sqrt{10}+g\sqrt{15}-h\sqrt{30})) \\ &= r_5(a-b\sqrt{2}-c\sqrt{3}+d\sqrt{5}+e\sqrt{6}-f\sqrt{10}-g\sqrt{15}+h\sqrt{30}) \\ &= a-b\sqrt{2}-c\sqrt{3}-d\sqrt{5}+e\sqrt{6}+f\sqrt{10}+g\sqrt{15}-h\sqrt{30})\end{aligned}$$

$$= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{5} + e\sqrt{6} + f\sqrt{10} + g\sqrt{15} + h\sqrt{30}$$

وهذا يحدث إذا كان وفقط إذا كان : $b = c = d = h = 0$

أى أن الحقل الجزئى الثابت يكون :

$$\{a + e\sqrt{6} + f\sqrt{10} + g\sqrt{15} \mid a, e, f, g \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10})$$

(و) العنصر x تحت تأثير $\{r_2, r_3, r_5\}$ يصبح :

$$a - b\sqrt{2} - c\sqrt{3} - d\sqrt{5} - e\sqrt{6} - f\sqrt{10} - g\sqrt{15} - h\sqrt{30}$$

فلايجاد الحقل الجزئى الثابت هنا يجب أن يتحقق

$$b = c = d = e = f = g = h = 0$$

ويكون الحقل الجزئى الثابت هنا هو :

$$\{a \mid a \in \mathbb{Q}\} = \mathbb{Q}$$

مثال ٣٥ : عين قيم أوتومورفيزم فوربينيس σ_2 المعرف كالآتى :

$$\sigma_2 : F \to F$$
$$a \mapsto a^2$$

على جميع عناصر الحقل فى مثال ٨ من أمثلة متنوعة(١) .اوجد الحقل الثابت لـــ σ_2.

الحل : عناصر الحقل هى $\bar{0}, \bar{1}, \alpha, \bar{1} + \alpha$

$$\sigma_2(\bar{0}) = \overline{0^2} = \bar{0},$$
$$\sigma_2(\bar{1}) = \overline{1^2} = \bar{1},$$
$$\sigma_2(\alpha) = \alpha^2 = \bar{1} + \alpha,$$
$$\sigma_2(\bar{1} + \alpha) = \alpha$$

واضح أن الحقل الثابت هو $\mathbb{Z}_2$.

مثال ٣٦ : عين قيم أوتومورفيزم فوربينيس σ_3 المعرف كالآتى :

$$\sigma_3 : F \to F$$
$$a \mapsto a^3$$

على جميع عناصر الحقل المنتهى التسعة المعطى فى تمرين (٢) من تمارين عامة (١) .

واوجد الحقل الثابت لـــ σ_3.

<u>الحل</u> : عناصر الحقل هى :

$\bar{0}$ ، $\bar{1}$ ، $\bar{2}$ ، α ، $\bar{2}\alpha$ ، $\bar{1}+\alpha$ ، $\bar{1}+\bar{2}\alpha$ ، $\bar{2}+\alpha$ ، $\bar{2}+\bar{2}\alpha$

ونلاحظ أن $\alpha^2+\bar{1}=\bar{0}$ ، ومن ثم فإن : $\alpha^3+\alpha=\bar{0}$ ، أى أن $\alpha^3=-\alpha=\bar{2}\alpha$.

والآن :

$$\sigma_3(\bar{0})=\bar{0}, \sigma_3(\bar{1})=\bar{1}, \sigma_3(\bar{2})=\bar{8}=\bar{2},$$

$$\sigma_3(\alpha)=\alpha^3=\bar{2}\alpha,$$

$$\sigma_3(\bar{2}\alpha)=\bar{8}\alpha^3=\bar{2}.\bar{2}\alpha=\bar{4}\alpha=\alpha$$

$$\sigma_3(\bar{1}+\alpha)=(\bar{1}+\alpha)^3=\overline{1^3}+3.\overline{1^2}.\alpha+3.\bar{1}.\alpha^2+\alpha^3=\bar{1}+\bar{0}+\bar{0}+\alpha^3=\bar{1}+\bar{2}\alpha.$$

$$\sigma_3(\bar{1}+\bar{2}\alpha)=(\bar{1}+\bar{2}\alpha)^3=\overline{1^3}+3.\overline{1^2}.\bar{2}\alpha+3.1(\bar{2}\alpha)^2+(\bar{2}\alpha)^3$$
$$=\bar{1}+\bar{8}\alpha^3=\bar{1}+\bar{2}.\bar{2}\alpha=\bar{1}+\bar{4}\alpha=\bar{1}+\alpha$$

$$\sigma_3(\bar{2}+\alpha)=(\bar{2}+\alpha)^3=\overline{2^3}+3.\overline{2^2}\alpha+3.\bar{2}.\alpha^2+\alpha^3=\bar{8}+\alpha^3=\bar{2}+\bar{2}\alpha.$$

$$\sigma_3(\bar{2}+\bar{2}\alpha)=\overline{2^3}+3.\overline{2^2}.\bar{2}\alpha+3.\bar{2}.(\bar{2}\alpha)^2+(\bar{2}\alpha)^3=\bar{8}+\bar{8}\alpha^3$$
$$=\bar{2}+\bar{2}.\bar{2}\alpha=\bar{2}+\bar{4}\alpha=\bar{2}+\alpha$$

واضح أن الحقل الثابت هو $\mathbb{Z}_3$

<u>مثال ٣٧</u> : بالإشارة إلى المثال ٣٢ السابق :

(أ) برهن على أن كل الأوتومورفيزمات r_2 ، r_3 ، r_5 من الرتبة 2 فى $Aut(E;\mathbb{Q})$

(ب) اوجد الزمرة الجزئية H فى $Aut(E;\mathbb{Q})$ المتولدة من r_2 ، r_3 ، r_5 . اكتب جدول الزمرة.

الحل :

(أ) $r_2^2 = r_3^2 = r_5^2 = 1$. أى أن رتبة أى أوتومورفيزم منها هو 2 .

(ب) $H = \{1, r_2, r_3, r_5, r_2 o r_3, r_2 o r_5, r_3 o r_5, r_2 o r_3 o r_5\}$

واضح أن الزمرة إبدالية ، وكل عناصرها من الرتبة 2 ، وبالتالى فإن H تكون متشاكلة (أيزومورفية) مع $(\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2, +)$. وهى الزمرة $\{1, r_2\} \otimes \{1, r_3\} \otimes \{1, r_5\}$

مثال ٣٨ : هل $Ord(G(E/F))$ ضربية للأبراج المنتهية ذات الامتدادات المنتهية أى أنه يكون

$$Ord(G(K/F)) = Ord(G(K/E)) Ord(G(E/F))$$

الحل : ليس هذا صحيحاً بالضرورة . مثال مضاد .

$$Ord(G(\mathbb{Q}(\sqrt[3]{2}; i\sqrt{3})/\mathbb{Q}) = 6 \neq 2 = 2.1 \quad = \quad Ord(G(\mathbb{Q}(\sqrt[3]{2}; i\sqrt{3})/\mathbb{Q}(\sqrt[3]{2}))).$$

٢-٢-٣

$$Ord(G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}))$$

(انظر تمرين ٢٠ فى تمارين عامة (٢))

ملحوظة : استخدمنا هنا $G(K/F)$ بدلاً من $Aut(K;F)$ ، كما جاء فى (٢-١-٢) .

مثال ٣٩ : برهن على أن

$$G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(i\sqrt{3})) \cong (\mathbb{Z}_3, +)$$

البرهان : $Ord(G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(i\sqrt{3}))) = 3$ (تمرين ٢٠ فى تمارين عامة (٢)) ، وبالتالى فإن $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(i\sqrt{3}))$ دائرية من الرتبة 3 ، وينتج المطلوب مباشرة من نظرية تفصيل الزمر الدائرية .

مثال ٤٠ : حدد أى التقارير الآتية يكون صحيحاً وأيها خاطئاً :

(أ) كل امتداد منته لكل حقل F يكون قابلاً للانفصال على F

(ب) كل امتداد منته لكل حقل منته F يكون قابلاً للانفصال (على F)

(جـ) كل حقل مميزه يساوى الصفر يكون تاماً

(د) كل كثيرة حدود من درجة n على أى حقل F يكون لها دائماً n من الأصفار المختلفة فى $\overline{F}$

(هـ) كل كثيرة حدود غير قابلة للتحليل (للتبسيط) من درجة n معرفة على كل حقل تام F يكون لها دائماً n من الأصفار المختلفة فى $\overline{F}$

(و) كل كثيرة حدود من درجة n معرفة على كل حقل تام F يكون لها دائماً n من الأصفار المختلفة فى $\overline{F}$

(ز) كل حقل مغلق جبرياً يكون تاماً

(ح) كل حقل F له امتداد جبرى تام E

(ط) إذا كان E امتداداً منتهياً قابلاً للانفصال حقل تشقيق لـ F فإن :

$Ord\,(Aut\,(E\,;F)) = [E : F]$

(ى) إذا كان E امتداداً منتهياً وحقل تشقيق لـ F فإن $Ord\,(Aut\,(E;F))$ يقسم $[E : F]$

__الحل__ : التقارير (أ) ، (د) ، (و) خاطئة . باقى التقارير صائبة .

__مثال ٤١__ : اضرب مثالاً لـ $f \in \mathbb{Q}[X]$ بحيث لا يكون لها أصفار فى $\mathbb{Q}$ ، ولكن أصفارها فى $\mathbb{C}$ كلها لها التكرار 2 . وضح كيف يتسق هذا مع كون $\mathbb{Q}$ تاماً

__الحل__ : $f := (X^2+1)^2 = X^4 + 2X^2 + 1$ تحقق المطلوب . كلا عاملى f غير قابل للتحليل فى $\mathbb{Q}[X]$ ، له صفر بسيط فى حقل تشقيقه . وهذا يتفق مع كون $\mathbb{Q}$ تاماً

__مثال ٤٢__ : برهن على أن كل كثيرة حدود غير ثابتة وغير قابلة للتحليل (للتبسيط) f على حقل F مميزه الصفر تكون قابلة للانفصال

__البرهان__ : من التمهيدية (٢-٤-٧) : إذا كان مميز الحقل = الصفر فإنه يكون : f ليست ثابتة إذا كان وفقط إذا كان $D(f) \neq 0$ ومن النظرية (٢-٤-٦) : f غير القابلة للتحليل تكون قابلة للانفصال إذا كان وفقط إذا كان $D(f) \neq 0$ ، وينتج المطلوب مباشرة .

مثال ٤٣ : برهن على أن كل كثيرة حدود غير قابلة للتبسيط q معرفة على حقل F له المميز $p \neq 0$ تكون غير قابلة للانفصال إذا كان وفقط إذا كان أس كل حد من حدود q يقبل القسمة على p

البرهان : من التمهيدية (٢-٤-٧) : إذا كان مميز الحقل = $p \neq 0$ ، فإنه توجد كثيرة حدود $g \in F[X]$ بحيث يكون $f(=f(X)) = g(X^p)$ إذا كان وفقط إذا كان $Df = 0$. ومن النظرية (٢-٤-٦) f غير القابلة للتحليل تكون غير قابلة للانفصال إذا كان وفقط إذا كان $Df = 0$ ، فينتج المطلوب مباشرة .

مثال ٤٤: صف برنامجاً حسابياً ملائماً لتعيين إذا ما كانت $f \in F[X]$ لها صفر مكرر ، بدون إيجاد أصفار f

الحل : احسب القاسم المشترك الأعظم لـ f ، f' باستخدام خوارزمية القسمة (نظرية (٢-١-٦) فى نظرية الحلقات) . f سيكون لها صفر مكرر إذا كانت درجة القاسم المشترك الأعظم لـ f ، f' أكبر من الصفر

مثال ٤٥ : عين $\alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ بحيث يكون $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$. حقق بالتعويض المباشر أن $\sqrt{2}$ ، $\sqrt{3}$ يمكن أن يعبر عنهما ككثيرات حدود شكلية فى α ، معاملاتها فى $\mathbb{Q}$

الحل : من مثال ١٨ فى أمثلة متنوعة (١) رأينا أن : $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ ، أى أن $\alpha = \sqrt{2}+\sqrt{3}$. يمكن التعبير عن $\sqrt{2}$ ، $\sqrt{3}$ كما هو مطلوب كالآتى :

$$\sqrt{2} = \frac{1}{2}\alpha^3 - \frac{9}{2}\alpha,$$

$$\sqrt{3} = \frac{11}{2}\alpha - \frac{1}{2}\alpha^3$$

تحقق من ذلك . (توجد طرائق أخرى للتعبير عن $\sqrt{2}$ ، $\sqrt{3}$)

مثال ٤٦ : حدد أى التقارير الآتية صائباً وأيها خاطئاً :

(١) ربما يكون لزمرتين جزئيتين من زمرة جالوا الحقل الثابت نفسه

(٢) إذا كانت الحقول F ، E ، L ، K بحيث إن $F \subset E \subset L \subset K$ ، فإن $\lambda(E) \subset \lambda(L)$ حيث $\lambda(E)$ هى الزمرة الجزئية من $Aut(K;F)$ التى تترك E ثابتاً ، $\lambda(L)$ الزمرة الجزئية من $Aut(K;F)$ التى تترك L ثابتاً .

(٣) إذا كان K امتداداً منتهياً طبيعياً لـF ، فإن K امتداد منته طبيعى لــ E ، حيث $F \subset E \subset K$.

(٤) إذا كان امتدادان طبيعيان منتهيان لــ F هما E ، L لهما زمرتا جالوا متشاكلتين ، فإن $[E:F]=[L:F]$.

(٥) إذا كان E امتداداً طبيعياً منتهياً لــ F ، H زمرة جزئية طبيعية من $Aut(E;F)$ ، فإن الحقل الثابت فى E بــ H : E_H يكون امتداداً طبيعياً لــ F .

(٦) إذا كان E أى امتداد منته طبيعى بسيط لحقل F ، فإن زمرة جالوا $Aut(G;F)$ تكون زمرة بسيطة .

(٧) لا توجد زمرة جالوا بسيطة .

(٨) زمرة جالوا لامتداد منته لحقل منته تكون إبدالية .

(٩) أى امتداد E له الدرجة 2 على حقل F يكون امتداداً طبيعياً لــ F .

(١٠) أى امتداد E له الدرجة 2 على حقل F يكون امتداداً طبيعياً لــ F إذا كان مميز F لا يساوى 2 .

الحل : التقارير (٣) ، (٤) ، (٥) ، (٨) ، (١٠) صحيحة . باقى التقارير خاطئ .

مثال ٤٧ : ليكن $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$. K امتداد طبيعى لــ $\mathbb{Q}$. ولقد رأينا فى مثال (٢-١-٥) أنه يوجد أربعة اوتومورفيزمات لــ K تترك $\mathbb{Q}$ ثابتاً ، سنعيد ذكرها بإعطاء قيمها على أساس K على $\mathbb{Q}$ وهو $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$:

راسم الوحدة

φ_1 الذى يرسم $\sqrt{3}$ على $-\sqrt{3}$ ، $\sqrt{6}$ على $-\sqrt{6}$ ويترك $\mathbb{Q}(\sqrt{2})$ ثابتاً

φ_2 الذى يرسم $\sqrt{2}$ على $-\sqrt{2}$ ، $\sqrt{6}$ على $-\sqrt{6}$ ويترك $\mathbb{Q}(\sqrt{3})$ ثابتاً

φ_3 الذى يرسم $\sqrt{2}$ على $-\sqrt{2}$ ، $\sqrt{3}$ على $-\sqrt{3}$ ويترك $\mathbb{Q}(\sqrt{6})$ ثابتاً

ولقد رأينا أن $\{1,\varphi_1,\varphi_2,\varphi_3\}$ تشاكل زمرة كلاين الرباعية ، ونوضح فى الآتى تناظر الزمر الجزئية مع الحقول البينية الثابتة

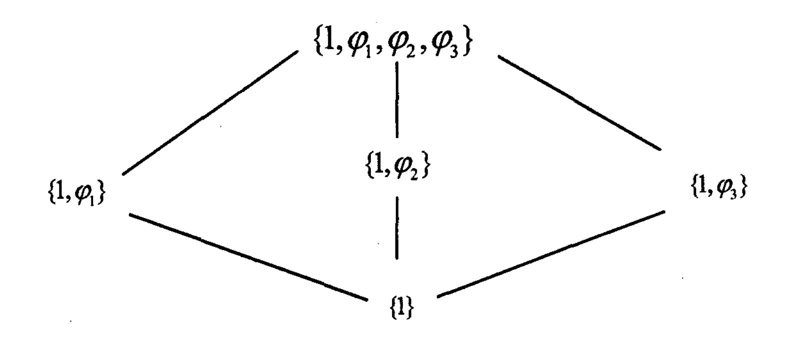
$\{1,\varphi_1,\varphi_2,\varphi_3\} \leftrightarrow \mathbb{Q}$ (1 راسم الوحدة)

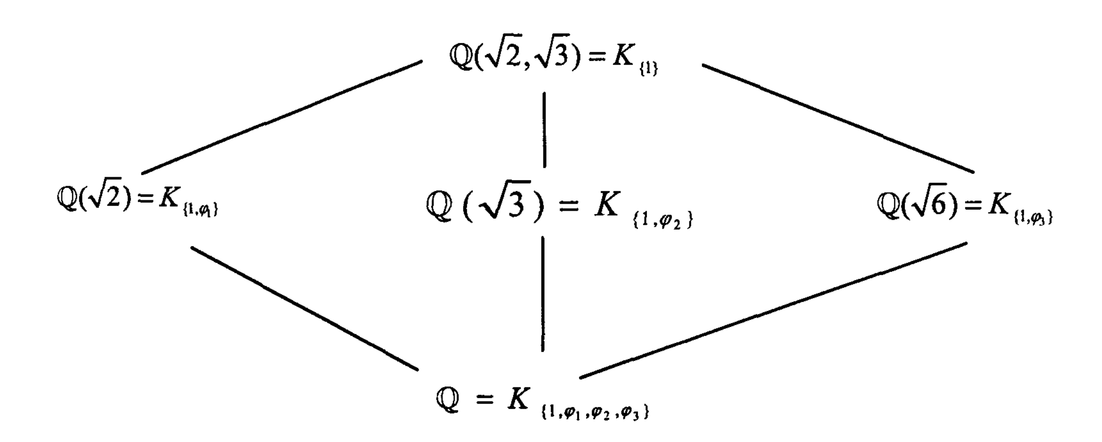
$$\{1,\varphi_1\} \leftrightarrow \mathbb{Q}(\sqrt{2})$$
$$\{1,\varphi_2\} \leftrightarrow \mathbb{Q}(\sqrt{3})$$
$$\{1,\varphi_3\} \leftrightarrow \mathbb{Q}(\sqrt{6})$$
$$\{1\} \leftrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$$

جميع الزمر الجزئية من الزمر الإبدالية $\{1,\varphi_1,\varphi_2,\varphi_3\}$ هى بالطبع طبيعية. وواضح أن جميع الحقول البينية هى امتدادات طبيعية لـــ $\mathbb{Q}$.

لاحظ أنه إذا كانت إحدى الزمر الجزئية محتواة فى أخرى ، فإن الزمرة الجزئية الأكبر منهما تناظر الحقل الأصغر من الحقلين الثابتين المناظرين . والسبب واضح ، فكلما كانت الزمرة الجزئية أكبر ، كانت الأوتومورفيزمات أكثر ، وبالتالى الحقل الثابت أصغر .

ونوضح فى الشكل أدناه شكلى "الشبكات" (lattices) المتناظرة للزمر الجزئية والحقول البينية . لاحظ مرة أخرى أن الزمر القريبة من القمة تناظر الحقول القريبة من القاع . أى أنه فى هذا المثال تبدو إحدى "الشبكات" (lattice) "معكوس" الأخرى ، أو أنها أديرت من أعلى إلى أسفل .





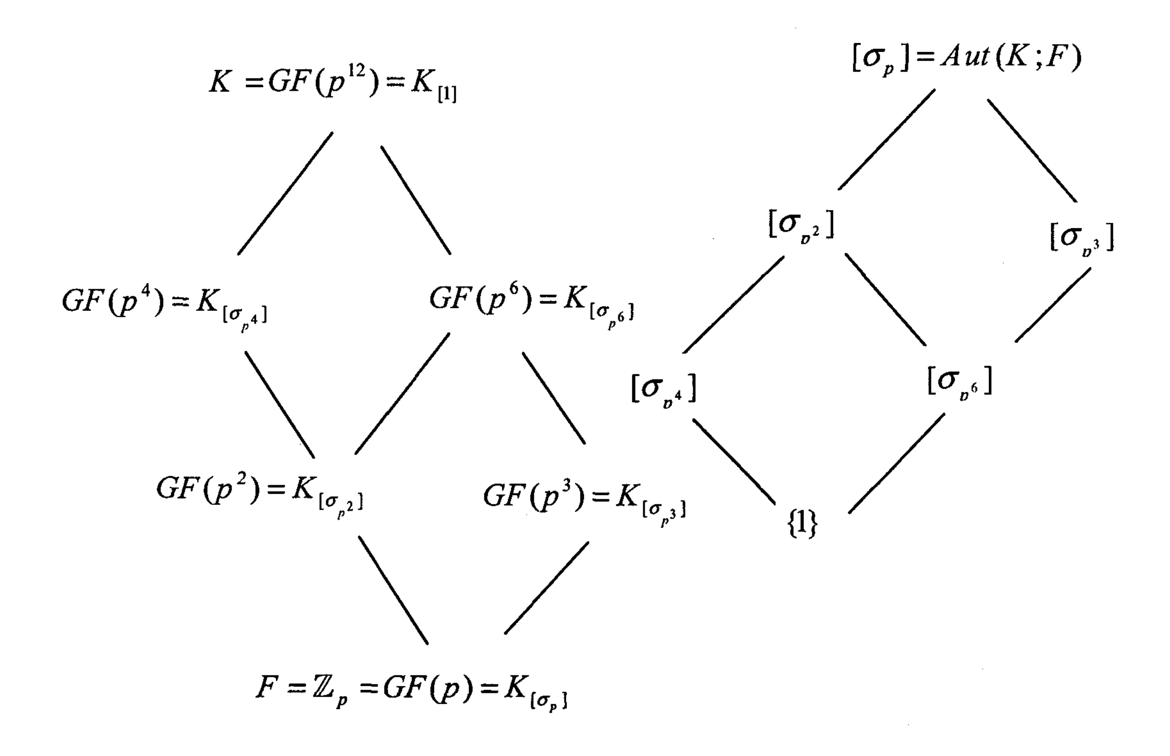
(K_H يعنى الحقل الثابت فى K بالزمرة الجزئية الطبيعية H)

<u>مثال ٤٨</u> : ليكن K امتداداً منتهياً من الدرجة n لحقل منته F ، عدد عناصره p^r . برهن على أن $Aut(G;F)$ دائرية من الرتبة n ، وتتولد بـــ σ_{p^r} حيث $\sigma_{p^r}(\alpha)=\alpha^{p^r}$ لجميع $\alpha\in K$.

<u>البرهان</u> : لأن أى حقل منته يكون تاماً فإن K يكون امتداداً قابلاً للانفصال لـــ F . لتكن رتبة F هى p^r ، وليكن $[K:F]=n$ ، وبهذا يكون عدد عناصر K هو p^{rn} . ويكون K هو حقل تشقيق كثيرة الحدود $X^{p^{rn}}-X$ على F . وبالتالى فإن K يكون امتداداً طبيعياً لـــ F .

والآن أحد الأوتومورفيزمات لـــ K التى تترك F ثابتاً هو σ_{p^r} ، حيث $\sigma_{p^r}(\alpha)=\alpha^{p^r}$ لجميع $\alpha \in K$. لاحظ أن $(\sigma_{p^r})^i(\alpha)=\alpha^{p^{ri}}$. ونظراً لأن كل كثيرة حدود من الدرجة p^{ri} يكون لها على الأكثر p^{ri} من الأصفار فى حقل ، فإن أصغر قوة (أس) لـــ σ_{p^r} التى من المحتمل أن تترك p^{rn} عنصراً (جميع عناصر K) ثابتة هى n . وبالتالى فإن رتبة العنصر σ_{p^r} فى $Aut(G;F)$ هى علي الأقل n . ولأن $Ord(Aut(G;F))=[K:F]=n$ ، فإن $Aut(G;F)$ يجب أن تكون دائرية ، وتتولد من σ_{p^r} . نهاية البرهان .

مثال ٤٩ : ليكن $F:=\mathbb{Z}_p$ ، $K:=GF(p^{12})$ ، ومن ثم فإن $[K:F]=12$ ((٢-٦-١٠) ، (٢-٢-٤)) . عندئذ فإن $Aut(K;F)$ تتشاكل مع الزمرة الدائرية $(\mathbb{Z}_{12},+)$. شكلا الشبكة للزمر الجزئية وللحقول البينية موضحان أدناه .مرة أخرى تبدو كل شبكة ليس فقط معكوس الأخرى ، ولكن كما لو كانت معكوس نفسها . هذه ليست دائماً الحال !



ونصف الزمر الجزئية فى $Aut(K;F) = [\sigma_p]$ بإعطاء المولدات ، وعلى سبيل المثال فإن :

$[\sigma_{p^4}] = \{1, \sigma_{p^4}, \sigma_{p^8}\}$.

<u>مثال ٥٠</u> : إذا كان لدينا امتدادات الحقول المنتهية الطبيعية كالآتى $F \subset E \subset K$ ، مع زمرة جالوا $Aut(K;F)$ فإننا نعنى بـــ $\lambda(E)$ الزمرة الجزئية من $Aut(K;F)$ التى تترك E ثابتاً . وليكن $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. والآن املأ الفراغات الآتية :

(أ) $[K:\mathbb{Q}] = ---$ (ب) $Ord(Aut(K;\mathbb{Q})) = ---$

(جـ) $Ord(\lambda(\mathbb{Q})) = ---$ (د) $Ord(\lambda(\mathbb{Q}(\sqrt{2}, \sqrt{3}))) = ---$

(هـ) $Ord\,(\lambda(\mathbb{Q}(\sqrt{6}))) = ---$ (و) $Ord(\lambda(\mathbb{Q}(\sqrt{30}))) = ---$

(ز) $Ord\,(\lambda(\mathbb{Q}(\sqrt{2}+\sqrt{6}))) = ---$ (ح) $Ord\,(\lambda(K)) = ---$

الحل :

(أ) (مثال ٤٠ فى أمثلة متنوعة (١)) $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}] = 8$

(ب) $K \supset \mathbb{Q}$ امتداد جالوا ، وبالتالى فإن :

$$Ord\,(Aut\,(K;\mathbb{Q})) = [K:\mathbb{Q}] = 8$$

(جـ) جميع الأوتومورفيزمات فى $Aut\,(K;\mathbb{Q})$ تترك $\mathbb{Q}$ ثابتاً . إذن

$$Ord\,(\lambda(\mathbb{Q})) = 8$$

(د) $\lambda(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ تتكون من العنصرين 1 ، φ_3 حيث $\varphi_3(\sqrt{5}) = -\sqrt{5}$ ، $\varphi_3(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ حقل ثابت. أى أن

$$Ord\,(\lambda(\mathbb{Q}(\sqrt{2},\sqrt{3}))) = 2$$

(هـ) $\lambda(\mathbb{Q}(\sqrt{6}))$ تتكون من أربعة عناصر هى : 1 ، φ_3 (كما سبق تعريفها ، φ_4 المعرفة كالآتى : $\varphi_4(\sqrt{3}) = -\sqrt{3}, \varphi_4(\sqrt{2}) = -\sqrt{2}$ ، $\varphi_4(\mathbb{Q}(\sqrt{5}))$ حقل ثابت ، φ_7 معرفة كالآتى : $\varphi_7(\sqrt{2}) = -\sqrt{2}$ ، $\varphi_7(\sqrt{3}) = -\sqrt{3}$ ، $\varphi_7(\sqrt{5}) = -\sqrt{5}$ ، $\varphi_7(\mathbb{Q})$ حقل ثابت ، أى أن

$$Ord\,(\lambda(\mathbb{Q}(\sqrt{6}))) = 4$$

(و) $\lambda(\mathbb{Q}(\sqrt{30}))$ تتكون من أربعة عناصر هى : 1 ، φ_4 سبق تعريفها ، φ_5 المعرفة كالآتى : $\varphi_5(\sqrt{3}) = -\sqrt{3}$ ، $\varphi_5(\sqrt{5}) = -\sqrt{5}$ ، $\varphi_5(\mathbb{Q}(\sqrt{2}))$ حقل ثابت ، φ_6 المعرفة كالآتى : $\varphi_6(\sqrt{2}) = -\sqrt{2}$ ، $\varphi_6(\sqrt{5}) = -\sqrt{5}$ ، $\varphi_6(\mathbb{Q}(\sqrt{3}))$ حقل ثابت .

أى أن $Ord\,(\lambda(\mathbb{Q}(\sqrt{3}))) = 4$

(ز) $\lambda(\mathbb{Q}(\sqrt{2}+\sqrt{6}))$ تتكون من عنصرين هما 1 ، φ_3 ويكون $Ord(\lambda(\mathbb{Q}(\sqrt{2}+\sqrt{6})))=2$

(ح) $\lambda(K)$ تتكون من عنصر واحد هو 1 ، ويكون $Ord(\lambda(K))=1$

<u>مثال ٥١</u> : صف زمرة جالوا لكثيرة الحدود $X^4-1\in\mathbb{Q}[X]$ على $\mathbb{Q}$

<u>الحل</u> : حقل تشقيق $X^4-1\in\mathbb{Q}[X]$ هو $\mathbb{Q}(i)$ لأن :

$X^4-1=(X-1)(X+1)(X-i)(X+i)$ (كثيرة حدود قابلة للانفصال)

ومن حيث إن $[\mathbb{Q}(i):\mathbb{Q}]=2$ (لأن كثيرة الحدود الصغرى لـــ i على $\mathbb{Q}$ هى X^2+1

ودرجتها= 2 فمن (١-٥-٥) يكون $[\mathbb{Q}(i):\mathbb{Q}]=2$) ويكون $Ord(Aut(\mathbb{Q}(i);\mathbb{Q}))=2$.

1 أحد عنصرى $Aut(\mathbb{Q}(i);\mathbb{Q})$ ، العنصر الآخر يجب أن تكون رتبته2(رتبة عنصر فى

زمرة تقسم رتبة الزمرة) وبالتالى فإن العنصر الآخر هو φ حيث $\varphi(i)=-i$ ، $\varphi(\mathbb{Q})=\mathbb{Q}$

<u>مثال ٥٢</u> : صف مولداً للزمرة $Aut(GF(729);GF(9))$ وعين رتبته .

<u>الحل</u> :

$$Ord(Aut(GF(729);GF(9)))=Ord(Aut(GF(3^6),GF(3^2)))$$
$$=3$$

ومن مثال ٤٨ السابق يكون لدينا المولد σ_{3^2} المعرف كالآتى :

$$\sigma_{3^2}(x)=x^{3^2}=x^9 \qquad \forall x\in GF(729)$$

<u>مثال ٥٣</u> : اضرب مثالاً لامتدادين طبيعيين منتهيين K_1 ، K_2 على نفس الحقل F ،

بحيث إن K_1 ، K_2 ليسا متشاكلين ، لكن $Aut(K_1;F)\cong Aut(K_2;F)$

<u>الحل</u> : الامتدادان هما $\mathbb{Q}(\sqrt{2})\supset\mathbb{Q}$ ، $\mathbb{Q}(\sqrt{3})\supset\mathbb{Q}$. بينما

$$Aut(\mathbb{Q}(\sqrt{2});\mathbb{Q})\cong(\mathbb{Z}_2,+)\cong Aut(\mathbb{Q}(\sqrt{3});\mathbb{Q})$$

<u>مثال ٥٤</u> : عين زمرة جالوا للامتداد $\mathbb{Q}(\alpha)\supset\mathbb{Q}$ حيث $\alpha=e^{\frac{2\pi i}{3}}$

<u>الحل</u> :

$$e^{\frac{2\pi i}{3}} = \cos\frac{2\pi}{3} + i\,\sin\frac{2\pi}{3}$$
$$= -\frac{1}{2} + \frac{i}{2}\sqrt{3}$$

المطلوب تعيين الأوتومورفيزمات لـــ $K = \mathbb{Q}(-\frac{1}{2} + \frac{i}{2}\sqrt{3}) = \mathbb{Q}(i\sqrt{3})$

(تذكر أن $Aut(\mathbb{Q}(\alpha);\mathbb{Q}) = Aut(\mathbb{Q}(\alpha))$ حيث إن $\mathbb{Q}$ الحقل الأولى للحقل $\mathbb{Q}(\alpha)$. ملحوظة (٢-١-٣)) ، $\alpha = i\sqrt{3}$. إذا كان φ فى زمرة جالوا فإن :

$$-3 = \varphi(-3) = \varphi(i\sqrt{3})^2 = (\varphi(i\sqrt{3}))^2 \Rightarrow \varphi(i\sqrt{3}) = \pm i\sqrt{3}$$

إذن يوجد أوتومورفيزمان على الأكثر فى زمرة جالوا أحدهما 1 (راسم الوحدة) . نلاحظ أن $\{1, i\sqrt{3}\}$ أساس لـــ $\mathbb{Q}(\alpha)$ على $\mathbb{Q}$. بديهى أن $\varphi^2(1) = 1$ ، إذا كان $\varphi(i\sqrt{3}) = -i\sqrt{3}$ فإن :

$$\varphi^2(i\sqrt{3}) = \varphi(\varphi(i\sqrt{3})) = \varphi(-i\sqrt{3}) = i\sqrt{3}$$

أى أن $\varphi^2 = 1$. أى أن رتبة الأوتومورفيزم $\varphi(i\sqrt{3}) = -i\sqrt{3}$ ، $\varphi(x) = x$ لجميع $x \in \mathbb{Q}$ هى 2 . وبالتالى فإن زمرة جالوا هى $(\mathbb{Z}_2, +)$

<u>مثال ٥٥</u> : عين زمرة جالوا للامتداد $K \supset \mathbb{Q}$ ، إذا كان K هو حقل تشقيق كثيرة الحدود $X^4 - 3X^2 + 4 \in \mathbb{Q}[X]$ على $\mathbb{Q}$.

<u>الحل</u> : لإيجاد حقل تشقيق كثيرة الحدود $X^4 - 3X^2 + 4 \in \mathbb{Q}[X]$:

$$X^4 - 3X^2 + 4 = 0 \Rightarrow X^2 = \frac{3 \pm \sqrt{9-16}}{2} = \frac{3}{2} \pm \frac{\sqrt{7}}{2} i$$

والآن ليكن $X^2 = \frac{3}{2} + \frac{\sqrt{7}}{2} i$:

$$X=\sqrt{\frac{3}{2}+\frac{\sqrt{7}}{2}i}=x+iy\Rightarrow x^2+2ixy-y^2=\frac{3}{2}+\frac{\sqrt{7}}{2}i$$

$$\Rightarrow \left.\begin{matrix} x^2-y^2=\frac{3}{2}(1), \\ 2xy=\frac{\sqrt{7}}{2}(2) \end{matrix}\right\rangle \left.\begin{matrix} x^2-y^2=\frac{3}{2}, \\ 4x^2y^2=\frac{7}{4} \end{matrix}\right\rangle \left.\begin{matrix} x^4-2x^2y^2+y^4=\frac{9}{4} \\ 4x^2y^2=\frac{7}{4} \end{matrix}\right\rangle (x^2+y^2)^2=4$$

$$\Rightarrow x^2+y^2=2\underset{(1)}{\Rightarrow}2x^2=\frac{7}{2}\Rightarrow x=\pm\frac{\sqrt{7}}{2}\underset{(2)}{\Rightarrow}y=\pm\frac{1}{2}$$

$$\Rightarrow X=\sqrt{\frac{3}{2}+\frac{\sqrt{7}}{2}i}=\frac{\sqrt{7}}{2}+\frac{i}{2} \quad \text{أو} \quad -\frac{\sqrt{7}}{2}-\frac{i}{2}$$

بالمثل إذا كان $X^2=\frac{3}{2}-\frac{\sqrt{7}}{2}i$ فإن

$$X=\frac{\sqrt{7}}{2}-\frac{i}{2} \quad \text{أو} \quad -\frac{\sqrt{7}}{2}+\frac{i}{2}$$

إذن حقل تشقيق كثيرة الحدود $X^4-3X^2+4\in\mathbb{Q}[X]$ على $\mathbb{Q}$ هو $\mathbb{Q}(\sqrt{7},i)$

المطلوب تعيين الأوتومورفيزمات لـــ $K:=\mathbb{Q}(\sqrt{7},i)$

إذا كان φ فى زمرة جالوا فإن :

$$7=\varphi(7)=\varphi((\sqrt{7})^2)=(\varphi(\sqrt{7}))^2\Rightarrow\varphi(\sqrt{7})=\pm\sqrt{7}$$

$$-1=\varphi(-1)=\varphi(i^2)=\varphi(i)^2\Rightarrow\varphi(i)=\pm i$$

هناك أربعة أوتومورفيزمات فى زمرة جالوا :

$$\varphi_1:\varphi_1(\sqrt{7})=\sqrt{7},\varphi_1(i)=i,$$

$$\varphi_2:\varphi_2(\sqrt{7})=\sqrt{7},\varphi_2(i)=-i,$$

$$\varphi_3:\varphi_3(\sqrt{7})=-\sqrt{7},\varphi_3(i)=i,$$

$\varphi_4 : \varphi_4(\sqrt{7}) = -\sqrt{7}, \varphi_4(i) = -i,$

$\varphi_j(x) = x \quad \forall x \in \mathbb{Q}, j = 1,...,4$

ومن حيث إن $\{1, \sqrt{7}, i, \sqrt{7}i\}$ أساس للفراغ الخطى $\mathbb{Q}(\sqrt{7}, i)$ على $\mathbb{Q}$ ،

$$\varphi_j^2(c) = c \qquad \forall c \in \{1, \sqrt{7}, i, \sqrt{7}i\}, j = 1,...,4$$

فإنه لجميع $j = 1,...,4$ فإن $\varphi_j^2 = 1$ ، وينتج أن زمرة جالوا هى زمرة كلاين الرباعية ، أى تتشاكل مع $(\mathbb{Z}_2 \otimes \mathbb{Z}_2, +)$. راجع كذلك مثال (٢—١—٥)

مثال ٥٦ : ليكن K حقل تشقيق $X^3 - 2$ على $\mathbb{Q}$

(أ) صف عناصر $Aut(K; \mathbb{Q})$ الستة وذلك باعطاء قيمها (قيمهم) على $\sqrt[3]{2}$ ، $i\sqrt{3}$ (حقل التشقيق هو $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$)

(ب) مع أية زمرة تتشاكل الزمرة $Aut(K; \mathbb{Q})$ ؟

(جـ) ارسم شكل شبكتى الحقول الجزئية من K ، والزمر الجزئية من $Aut(K; \mathbb{Q})$ موضحاً تناظر الحقول البينية والزمر الجزئية .

الحل :

(أ)

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4}) = 0$$

$$\Rightarrow X = \sqrt[3]{2}, X = \frac{-\sqrt[3]{2} \pm \sqrt{\sqrt[3]{4} - 4\sqrt[3]{4}}}{2} = \frac{\sqrt[3]{2}[-1 \pm \sqrt{3}i]}{2}$$

بالرجوع إلى مثال ٦٦ فى امثلة متنوعة (١)

نلاحظ أن $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$ ومن حيث إنه امتداد جالوا (انظر (٢—٥—٤)) ، فإن :

$Ord(Aut(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}); \mathbb{Q})) = 6$ ، أى أن هناك ستة عناصر فى $Aut(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}); \mathbb{Q})$

كما نلاحظ أن

$$(\frac{-1+i\sqrt{3}}{2})^2 = \frac{1-2i\sqrt{3}-3}{4} = \frac{-1-i\sqrt{3}}{2},$$
$$(\frac{-1-i\sqrt{3}}{2})^2 = \frac{1+2i\sqrt{3}-3}{4} = \frac{-1+i\sqrt{3}}{2}$$

والآن :

φ_1 : the identity mapping : $\varphi_1(\sqrt[3]{2}) = \sqrt[3]{2}, \varphi_1(i\sqrt{3}) = i\sqrt{3}$

$$\varphi_2 : \varphi_2(\sqrt[3]{2}) = \sqrt[3]{2}(\frac{-1+i\sqrt{3}}{2}), \varphi_2(i\sqrt{3}) = i\sqrt{3}$$

$$\varphi_3 : \varphi_3(\sqrt[3]{2}) = \sqrt[3]{2}(\frac{-1-i\sqrt{3}}{2}), \varphi_3(i\sqrt{3}) = i\sqrt{3}$$

$$\varphi_4 : \varphi_4(\sqrt[3]{2}) = \sqrt[3]{2}, \varphi_4(i\sqrt{3}) = -i\sqrt{3}$$

$$\varphi_5 : \varphi_5(\sqrt[3]{2}) = \sqrt[3]{2}(\frac{-1+i\sqrt{3}}{2}), \varphi_5(i\sqrt{3}) = -i\sqrt{3}$$

$$\varphi_6 : \varphi_6(\sqrt[3]{2}) = \sqrt[3]{2}(\frac{-1-i\sqrt{3}}{2}), \varphi_6(i\sqrt{3}) = -i\sqrt{3}$$

لاحظ أن $\{\varphi_1, \varphi_2\}$ لاتكون زمرة جزئية من $Aut(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}), \mathbb{Q})$

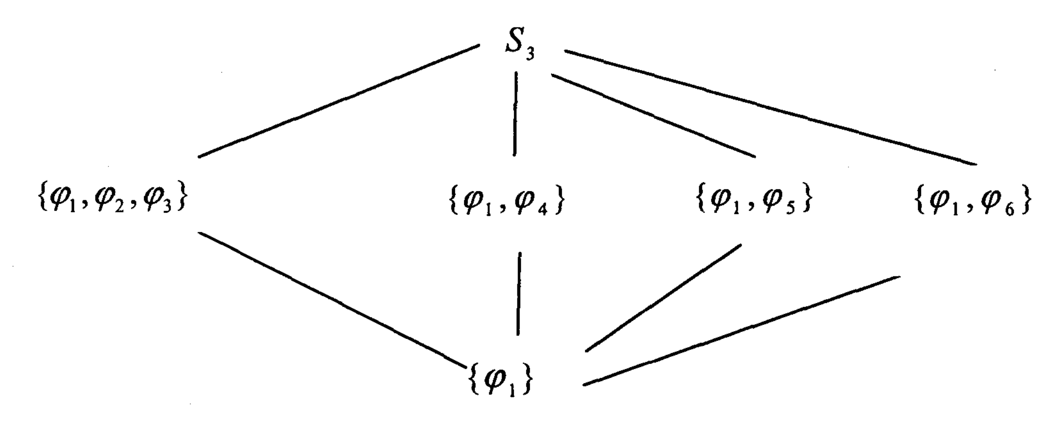
لأ ن:

$$\varphi_2^2(\sqrt[3]{2}) = \varphi_2(\varphi_2(\sqrt[3]{2})) = \varphi_2(\sqrt[3]{2}(\frac{-1+i\sqrt{3}}{2}))$$
$$= \varphi_2(\sqrt[3]{2})\varphi_2(\frac{-1+i\sqrt{3}}{2}) = \sqrt[3]{2}(\frac{-1+i\sqrt{3}}{2})(\frac{-1+i\sqrt{3}}{2})$$
$$= \sqrt[3]{2}\,\frac{1-2i\sqrt{3}-3}{4} = \frac{-\sqrt[3]{2}}{2}(1+i\sqrt{3})$$

أى أن $\varphi_2^2 \notin \{\varphi_1, \varphi_2\}$. بالمثل $\{\varphi_1, \varphi_3\}$ ليست زمرة جزئية من $Aut(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}), \mathbb{Q})$

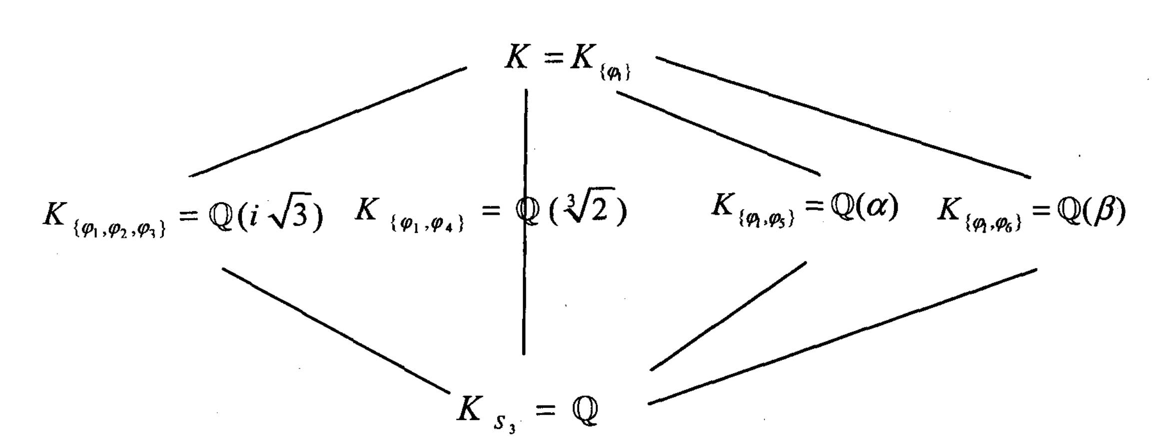
(ب) واضح أن رتبة φ_i حيث $i = 1, \dots, 6$ لاتساوى 6 ، وبالتالى فإن $Aut(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}), \mathbb{Q})$ لا تشاكل $\mathbb{Z}_6$ ، وبالتالى فهى تشاكل S_3 .

(جـ)



شبكة الزمر الجزئية

(K_H هو الحقل الثابت بـ H)



$$(\alpha = (\frac{-1 + i\sqrt{3}}{2})\sqrt[3]{2}, \beta = (\frac{-1 - i\sqrt{3}}{2})\sqrt[3]{2})$$

شبكة الحقول الجزئية

والتناظر المطلوب واضح .

<u>مثال ٥٧</u> : ليكن E امتداداً للحقل $\mathbb{Q}$. برهن على أن أى أوتومورفيزم لـ E يعمل على $\mathbb{Q}$ كأنه راسم الوحدة .

<u>البرهان</u> : ليكن φ أوتومورفيزماً على E . والآن :

$$\varphi(1)=1 \Rightarrow \varphi(n)=n \quad \forall n \in \mathbb{Z}$$

كذلك فإن :

$$1=\varphi(1)=\varphi(mm^{-1})=\varphi(m)\varphi(m^{-1}), \quad m \in \mathbb{Z}\setminus\{0\}$$
$$\Rightarrow \frac{1}{m}=\frac{1}{\varphi(m)}=\varphi(m^{-1})$$

وبالتالى فإن :

$$\varphi(\frac{n}{m})=\varphi(nm^{-1})=\varphi(n)\varphi(m^{-1})$$
$$=\frac{n}{m}, \qquad m \in \mathbb{Z}\setminus\{0\}, n \in \mathbb{Z}.$$

(قارن مع مثال ٣١ فى (١-٢-٨) فى نظرية الحلقات)

<u>مثال ٥٨</u> : اعتبر الامتداد $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$. من مثال ٥٧ السابق مباشرة أى أوتومورفيزم φ على $\mathbb{Q}(\sqrt[3]{2})$ يتعيين تماماً بمعرفة $\varphi(\sqrt[3]{2})$. والآن :

$$2=\varphi(2)=\varphi((\sqrt[3]{2})^3)=(\varphi(\sqrt[3]{2}))^3 \Rightarrow \varphi(\sqrt[3]{2}))^3-2=0$$
$$\Rightarrow (\varphi(\sqrt[3]{2})-\sqrt[3]{2})((\varphi(\sqrt[3]{2}))^2+\varphi(\sqrt[3]{2}).\sqrt[3]{2}+\sqrt[3]{4})=0$$

الحل الوحيد للمعادلة فى $\mathbb{Q}\,(\sqrt[3]{2})$ هو : $\qquad \varphi(\sqrt[3]{2})=\sqrt[3]{2}$

وبالتالى ومن مثال ٥٧ مرة اخرى فإن φ هو راسم الوحدة ، وتكون $Aut(\mathbb{Q}(\sqrt[3]{2});\mathbb{Q})$ من عنصر واحد هو راسم الوحدة، ويكون الحقل الثابت بـ $Aut(\mathbb{Q}(\sqrt[3]{2}))$ هو $\mathbb{Q}(\sqrt[3]{2})$.
(قارن مع مثال (٢-٢-٣))

<u>مثال ٥٩</u> : اعتبر الامتداد $\mathbb{Q}(\sqrt[4]{2},i) \supset \mathbb{Q}(i)$. أى أوتومورفيزم φ على $\mathbb{Q}(\sqrt[4]{2},i)$ مثبتا $\mathbb{Q}(i)$ يتعين تماما بـ $\varphi(\sqrt[4]{2})$. والآن :

$$2 = \varphi(2) = \varphi((\sqrt[4]{2})^4) = (\varphi(\sqrt[4]{2}))^4$$

$$\Rightarrow \varphi(\sqrt[4]{2}) = \sqrt[4]{2}(\cos\frac{0+2k\pi}{4} + i\sin\frac{0+2k\pi}{4}), k = 0,1,2,3$$

أى أن هناك أربعة أوتومورفيزمات ممكنة لـ $\mathbb{Q}(\sqrt[4]{2}, i)$ تثبت $\mathbb{Q}(i)$.

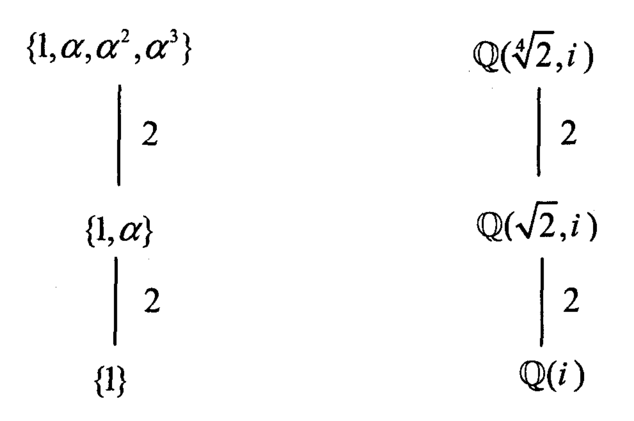
إذا عرفنا φ بالكيفية الآتية : $\varphi(i) = i$ ، $\varphi(\sqrt[4]{2}) = i\sqrt[4]{2}$ ، عندئذ فإن :

$\varphi \in Aut(\mathbb{Q}(\sqrt[4]{2}, i); \mathbb{Q}(i))$ ، $Ord(\varphi) = 4$. وبالتالى فإن $Aut(\mathbb{Q}(\sqrt[4]{2}, i); \mathbb{Q}(i))$ تكون زمرة دائرية رتبتها 4 . الحقل الثابت لـ $\{1, \varphi^2\}$ هو $\mathbb{Q}(\sqrt{2}, i)$ لأن :

$$\varphi^2(i) = \varphi(\varphi(i)) = \varphi(i) = i,$$

$$\begin{aligned}\varphi^2(\sqrt{2}) &= \varphi(\varphi(\sqrt[4]{2}\sqrt[4]{2})) = \varphi(\varphi(\sqrt[4]{2}).\varphi(\sqrt[4]{2})) \\ &= \varphi(i\sqrt[4]{2}.i\sqrt[4]{2}) = \varphi(i)\varphi(i)\varphi(\sqrt[4]{2})\varphi(\sqrt[4]{2}) \\ &= i.i.i\sqrt[4]{2}.i\sqrt[4]{2} = \sqrt{2}\end{aligned}$$

شبكة الزمر الجزئية من $Aut(\mathbb{Q}(\sqrt[4]{2}, i); \mathbb{Q}(i))$ وشبكة الحقول البينية بين $\mathbb{Q}(\sqrt[4]{2}, i)$ ، $\mathbb{Q}(i)$ موضحتان أدناه . الأعداد الصحيحة على الخطوط فى شبكة الزمر الجزئية توضح دليل الزمرة الجزئية فى الزمرة أعلاها ، والأعداد الصحيحة على الخطوط فى شبكة الحقول توضح درجة امتداد الحقل فى الحقل أدناه



مثال ٦٠ : ليكن F حقلاً له المميز 0 (صفر) . إذا كان K هو حقل تشقيق $X^n - 1$ على F ، فبرهن على أن $Aut(K;F)$ زمرة إبدالية .

البرهان :

$$X^n - 1 = 0 \Rightarrow X = (\cos 0 + i \sin 0)^{1/n}$$
$$= \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}, k = 0,1,\dots,n-1$$

ليكن $X_1 = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$. تعطى عناصر $Aut(K;F)$ حيث $K = \mathbb{Q}(X_1)$ كالآتى :

$$\sigma_j \in Aut(K;F), \sigma_j(X_1) = X_1^j$$

وبالتالى فإن :

$$(\sigma_{j_1} o \sigma_{j_2})(X_1) = \sigma_{j_1}(X_1^{j_2}) = X_1^{j_1 j_2}$$
$$= \sigma_{j_2}(X_1^{j_1}) = (\sigma_{j_2} o \sigma_{j_1})(X_1)$$

وبالتالى فإن $\sigma_{j_1} o \sigma_{j_2} = \sigma_{j_2} o \sigma_{j_1}$ وينتج المطلوب مباشرة .

مثال ٦١ : عين فصل التشاكل (isomorphism class) للزمرة $Aut(GF(64);GF(2))$

الحل : المطلوب تعيين $Aut(GF(2^6);GF(2))$

من (٢-٦-١٠) $GF(2^6) \supset GF(2)$ امتداد جالوا ومن ثم فإن :

$$Ord(Aut(GF(2^6);GF(2))) = [GF(2^6):GF(2)] = 6$$

من (٢-١-٣) : $Aut(GF(2^6)) = Aut(GF(2^6),GF(2))$ ، ومن (٢-٦-١٠) $Aut(GF(2^6))$ دائرية يولدها هومومورفيزم فوربينيس ، ومن ثم فإن

$$Aut(GF(2^6);GF(2)) \cong \mathbb{Z}_6$$

مثال ٦٢ : عين فصل التشاكل للزمرة $Aut(GF(729);GF(9))$

<u>الحل</u>: المطلوب تعيين فصل التشاكل للزمرة : $Aut(GF(3^6);GF(3^2))$

لدينا

$$[GF(3^6):GF(3)] \quad = \quad [GF(3^6):GF(3^2)].[GF(3^2):GF(3)]$$

نظرية الدرجة

$GF(3^2) \supset GF(3)$ ، $GF(3^6) \supset GF(3)$ امتدادا جالوا من (٢-٦-١٠) ومن ثم فإن

$$2 = [GF(3^2):GF(3)] = Ord(Aut(GF(3^2);GF(3)))$$

كذلك فإن :

$$6 = [GF(3^6):GF(3)] = Ord(Aut(GF(3^6);GF(3)))$$

ومن ثم فإن

$$Ord(Aut(GF(3^2);GF(3))) = Ord(Aut(GF(3^6);GF(3))) / Ord(Aut(GF(3^6);GF(3^2)))$$

$$\Rightarrow 2 = 6 \big/ Ord(Aut(GF(3^6);GF(3^2)))$$

أى أن $Ord(Aut(GF(3^6);GF(3^2))) = 3$

وبالتالى فإن $Aut(GF(3^6);GF(3^2)) \cong \mathbb{Z}_3$

<u>مثال ٦٣</u> : ليكن E حقل تشقيق كثيرة الحدود X^4+1 على $\mathbb{Q}$.

اوجد $Aut(E;\mathbb{Q})$. كذلك أوجد الحقول الجزئية من E . واوجد أوتومورفيزمات E التى تكون الحقول الثابتة لها هى $\mathbb{Q}(\sqrt{2})$ ، $\mathbb{Q}(\sqrt{-2})$ ، $\mathbb{Q}(i)$. هل هناك أوتومورفيزم حقله الثابت $\mathbb{Q}$ ؟

<u>الحل</u> : لاحظ أن : $X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$

ومن ثم فإن أصفار X^4+1 هى :

$$X = \frac{\sqrt{2}\pm\sqrt{2-4}}{2}, \frac{-\sqrt{2}\pm\sqrt{2-4}}{2} = \frac{\pm\sqrt{2}\pm\sqrt{2}i}{2},$$

وبالتالى فإن حقل تشقيق X^4+1 على $\mathbb{Q}$ هو $\mathbb{Q}(\sqrt{2},i)$

وتكون $Aut(E;\mathbb{Q}) = Aut(\mathbb{Q}(\sqrt{2},i);\mathbb{Q})$

ويكون $Ord(Aut(E;\mathbb{Q})) = [E:\mathbb{Q}] = 4$ ((١-٥-٥) ، (٢-٢-٤)) وتكون عناصر الزمرة $Aut(E;\mathbb{Q})$ هى : 1 راسم الوحدة ، الحقل الثابت له E ،

$$\varphi_1, \varphi_1(\sqrt{2}) = -\sqrt{2}, \varphi_1(i) = i$$

أى له الحقل الثابت $\mathbb{Q}(i)$ ،

$$\varphi_2, \varphi_2(\sqrt{2}) = \sqrt{2}, \varphi_2(i) = -i$$

أى له الحقل الثابت $\mathbb{Q}(\sqrt{2})$ ،

$$\varphi_3 = \varphi_1 o \varphi_2 \Rightarrow \varphi_3(\sqrt{2}) = -\sqrt{2}, \varphi_3(i) = -i$$

ويكون

$$\begin{aligned}\varphi_3(\sqrt{-2}) &= \varphi_3(i\sqrt{2}) \\ &= \varphi_3(i)\varphi_3(\sqrt{2}) = -i(-\sqrt{2}) = i\sqrt{2} = \sqrt{-2}\end{aligned}$$

ويكون الحقل الثابت $\mathbb{Q}(\sqrt{-2})$

ولايوجد أوتومورفيزم حقله الثابت $\mathbb{Q}$

الحقول الجزئية الفعلية هى : $\mathbb{Q}(\sqrt{2})$ ، $\mathbb{Q}(i)$ ، $\mathbb{Q}(\sqrt{-2})$ ، $\mathbb{Q}$

<u>مثال ٦٤</u> : لتكن $f \in F[X]$ ، ولتكن أصفار f هى a_1 ، a_2 ، ... ، a_n . إذا كان $K = F(a_1, a_2, \dots, a_n)$ ، فبرهن على أن $Aut(K;F)$ تشاكل زمرة أوتومورفيزمات لـــ $a_i's$.

<u>البرهان</u> : يكفى أن نبرهن على أن أى عنصر فى $Aut(K;F)$ يعرف تبديلاً على الـــ $a_i's$. ليكن $\sigma \in Aut(K;F)$ ، ونكتب :

$$f = c_n X^n + c_{n-1}X^{n-1} + \dots + c_0 = c_n(X-a_1)(X-a_2)\dots(X-a_n),$$

$$c_n, c_{n-1}, \dots, c_0 \in F\ ,\ a_1, a_2, \dots, a_n \in K$$

ومن ثم فإن :

$$f = \sigma(f) = \sigma(c_n)\sigma(X - a_1)\sigma(X - a_2)...\sigma(X - a_n)$$
$$= \sigma(c_n)(X - \sigma(a_1))(X - \sigma(a_2))...(X - \sigma(a_n))$$

$f(a_i) = 0$ (لأن a_i صفر لـــ f) يقتضى أن :

$$0 = f(a_i) = \sigma(c_n)(a_i - \sigma(a_1))(a_i - \sigma(a_2))...(a_i - \sigma(a_n))$$

ومن ثم فإن : $a_i = \sigma(a_j)$ لبعض j

أى أن σ تبدل الـــ $a_i's$.

مثال ٦٥ : ليكن $\omega = \cos\frac{360^\circ}{7} + i\sin\frac{360^\circ}{7}$ بحيث إن $\omega^7 = 1$ ، ولنعتبر الحقل $\mathbb{Q}(\omega)$

كم عدد الحقول الجزئية من $\mathbb{Q}(\omega)$ ، وماهى ؟

الحل : أولاً لاحظ أن $\mathbb{Q}(\omega)$ هو حقل تشقيق $X^7 - 1$ على $\mathbb{Q}$ وهى قابلة للانفصال وبالتالى فإن لدينا امتداد جالوا . والآن ليكن φ أوتومورفيزم بحيث إن :

$$\varphi(\omega) = \omega^3 \Rightarrow \varphi^2(\omega) = \varphi(\varphi(\omega)) = \varphi(e^{\frac{2\pi i}{7}})^3 = \varphi(e^{\frac{6\pi i}{7}}) = e^{\frac{18\pi i}{7}} = e^{\frac{4\pi i}{7}}$$

$$\Rightarrow \varphi^3(\omega) = \varphi(\varphi^2(\omega)) = \varphi(e^{\frac{4\pi i}{7}}) = e^{\frac{12\pi i}{7}}$$

$$\Rightarrow \varphi^4(\omega) = \varphi(\varphi^3(\omega)) = \varphi(e^{\frac{12\pi i}{7}}) = e^{\frac{36\pi i}{7}} = e^{\frac{8\pi i}{7}}$$

$$\Rightarrow \varphi^5(\omega) = \varphi(\varphi^4(\omega)) = e^{\frac{24\pi i}{7}} = e^{\frac{10\pi i}{7}}$$

$$\Rightarrow \varphi^6(\omega) = \varphi(\varphi^5(\omega)) = e^{\frac{30\pi i}{7}} = e^{\frac{2\pi i}{7}} = \omega$$

أو بخطوات أسرع :

$$\varphi^6(\omega) = \varphi^5(\varphi(\omega)) = \varphi^5(\omega^3) = \varphi^4(\varphi(\omega^3)) = \varphi^4(\omega^9) = \varphi^4(\omega^2)$$
$$= \varphi^3(\varphi(\omega^2)) = \varphi^3(\omega^6) = \varphi^2(\varphi(\omega^6)) = \varphi^2(\omega^{18}) = \varphi^2(\omega^4)$$
$$= \varphi(\varphi(\omega^4)) = \varphi(\omega^{12}) = \varphi(\omega^5) = \omega^{15} = \omega$$

وهذا يقتضى أن $\varphi^6 = 1$ أى أن رتبة (φ) هى 6

ومن حيث إن رتبة أى عنصر فى زمرة تقسم رتبة الزمرة ((١-١١-٩) فى نظرية الزمر) ، ومن حيث إن لدينا امتداد جالوا فإنه ينتج أن :

$$[\mathbb{Q}(\omega):\mathbb{Q}] = Ord\,(Aut\,(Q\,(\omega);\mathbb{Q})) \geq 6$$

كذلك فإن لدينا :

$$X^7 - 1 = (X-1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$$

ومن حيث إن ω صفر لكثيرة الحدود $X^7 - 1$ ، $\omega - 1 \neq 0$ فإن

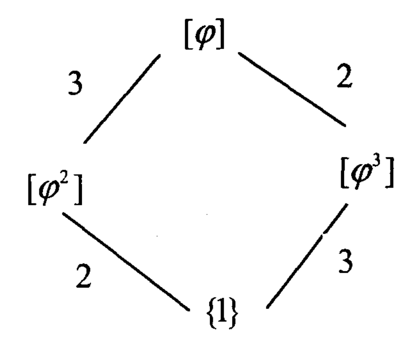
$$\omega^6 + \omega^5 + \omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$$

أى أن $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ هى كثيرة الحدود الصغرى من ω على $\mathbb{Q}$

فإن هذا يقتضى من (١-٥-٥) أن :

$$Ord\,(Aut\,(\mathbb{Q}(\omega);\mathbb{Q})) = [\mathbb{Q}((\omega):\mathbb{Q}] = 6$$

وهكذا فإن $Aut\,(\mathbb{Q}(\omega);\mathbb{Q}))$ دائرية ورتبتها 6 . ويمكن رسم شبكة الزمر الجزئية لـ $Aut\,(\mathbb{Q}(\omega);\mathbb{Q}))$ ، كما يتضح أدناه :



وهذا يعنى أن $\mathbb{Q}(\omega)$ يحتوى على امتدادين فعليين على $\mathbb{Q}$ أحدهما درجته 3 ، والآخر درجته 2 .

ونلاحظ أن $\omega + \omega^6$ ثابت تحت تأثير φ^3 ، لأن :

$$\varphi^3(\omega+\omega^6)=\varphi^2(\varphi(\omega+\omega^6)=\varphi^2(\varphi(\omega)+\varphi(\omega^6))$$
$$=\varphi^2(\omega^3+\omega^{18})=\varphi(\varphi(\omega^3+\omega^4))=\varphi(\omega^9+\omega^{12})=\varphi(\omega^2+\omega^5)$$
$$=\omega^6+\omega^{15}=\omega+\omega^6$$

وبالتالى فإن $\mathbb{Q}(\omega)_{[\varphi^3]} \supset \mathbb{Q}(\omega+\omega^6) \underset{\neq}{\supseteq} \mathbb{Q}$. ولأن $[\mathbb{Q}(\omega)_{[\varphi^3]}:\mathbb{Q}]=3$

(لماذا ؟) ولأن $[\mathbb{Q}(\omega+\omega^6):\mathbb{Q}]$ يقسم $[\mathbb{Q}(\omega)_{[\varphi^3]}:\mathbb{Q}]$ ولأن $\mathbb{Q}\neq\mathbb{Q}(\omega+\omega^6)$ فإن

$\mathbb{Q}(\omega+\omega^6)=\mathbb{Q}(\omega)_{[\omega^3]}$. (نعنى بـــ $\mathbb{Q}(\omega)_{[\varphi^3]}$ الحقل الثابت فى $\mathbb{Q}(\omega)$ تحت تأثير $[\varphi^3]$)

كذلك فإن $\omega^3+\omega^5+\omega^6$ ثابت تحت تأثير φ^2 لأن :

$$\varphi^2(\omega^3+\omega^5+\omega^6)=\varphi(\varphi(\omega^3+\omega^5+\omega^6))=\varphi(\varphi(\omega^3)+\varphi(\omega^5)+\varphi(\omega^6))$$
$$=\varphi(\omega^9+\omega^{15}+\omega^{18})=\varphi(\omega^2+\omega+\omega^4)=\varphi(\omega^2)+\varphi(\omega)+\varphi(\omega^4)$$
$$=\omega^6+\omega^3+\omega^{12}=\omega^3+\omega^5+\omega^6$$

وبالتالى فإن : $\mathbb{Q}(\omega)_{[\varphi^2]} \supset \mathbb{Q}(\omega^3+\omega^5+\omega^6) \underset{\neq}{\supseteq} \mathbb{Q}$. ولأن $[\mathbb{Q}(\omega)_{[\varphi^2]}:\mathbb{Q}]=2$

(لماذا ؟) ولأن $[\mathbb{Q}(\omega^3+\omega^5+\omega^6):\mathbb{Q}]$ يقسم $[\mathbb{Q}(\omega)_{[\varphi^2]}:\mathbb{Q}]$ ولأن

$\mathbb{Q}\neq\mathbb{Q}(\omega^3+\omega^5+\omega^6)$ فإن $\mathbb{Q}(\omega^3+\omega^5+\omega^6)=\mathbb{Q}(\omega)_{[\varphi^2]}$. وبهذا نكون

قد أوجدنا جميع الحقول الجزئية من $\mathbb{Q}(\omega)$.

<u>مثال ٦٦</u> : بالرجوع إلى مثال ٢٤ (جـــ) من أمثلة متنوعة (٢) اوجد الجذور البدائية الخمس عشرية.

<u>الحل</u> : وجدنا من قبل أن عدد الجذور هو 8 . والمطلوب تعيينها . نجرب $\bar{2}$ كمولد لـــ $(GF(31))^*$ أى $\mathbb{Z}_{31}^*$. من حيث إن رتبة $\mathbb{Z}_{31}^*$ هى 30 ، فرتبة $\bar{2}$ تكون قاسماً لـــ 30 أى هى 2 أو 3 أو 5 أو 6 أو 10 أو 15 أو 30 .

$\overline{2^2}=\bar{4}$ ، $\overline{2^3}=\bar{8}$ ، $\overline{2^5}=\bar{1}$ وبالتالى فإن $\bar{2}$ لايمكن أن يكون مولداً لـــ $\mathbb{Z}_{31}^*$.

نجرب $\bar{3}:\bar{9}=(\overline{3^2}=)^2(\bar{3})$ ، $\overline{27}=\overline{3^3}$ ، $\overline{26}=\overline{3^5}$ ، $\overline{16}=\overline{3^6}$ ، $\overline{25}=\overline{3^{10}}$ ،

أى $\overline{3^{15}}=\overline{30}$

أن $\overline{3^{30}}=\bar{1}$ (حسبنا قوى $\bar{3}$ التى تكون قاسماً لرتبة الزمرة $\mathbb{Z}_{31}^*$ كما فعلنا مع $\bar{2}$) .

أى أن $\bar{3}$ مولد لـــ $\mathbb{Z}_{31}^*$. وبالتالى تكون الجذور المطلوبة هى : $\overline{3^2}$ ، $\overline{3^4}$ ، $\overline{3^8}$ ، $\overline{3^{14}}$ ، $\overline{3^{16}}$ ، $\overline{3^{22}}$ ، $\overline{3^{26}}$ ، $\overline{3^{28}}$.

تمارين عامة (٢)

(١) عين أى كثيرات الحدود الآتية تعتبر قابلة للانفصال على الحقول الموضحة :

t^3+1 ، t^2+2t-1 ، $t^6+t^5+t^4+t^3+t^2+t+1$ ، $7t^5+t-1$ ؛

$\mathbb{Q}$ ، $\mathbb{C}$ ، $\mathbb{Z}_2$ ، $\mathbb{Z}_3$ ، $\mathbb{Z}_5$ ، $\mathbb{Z}_7$ ، $\mathbb{Z}_{19}$.

(٢) برهن على أن أى امتداد درجته 2 يكون طبيعياً . هل هذا صحيح بالنسبة لأية درجة >2 ؟

(٣) ليكن K هو الحقل فى مثال ٥٦ من تمارين متنوعة (١) ، وليكن P هو حقله الأولى . ما زمرة جالوا $Aut(K;P)$ ؟ هل الراسمان $Aut(K;\ \ )$ ، $Fix(K;\ \ )$ فى (٢-٢-٤) تناظران أحاديان هنا ؟

(٤) أنشئ حقلاً مكوناً من 16 عنصراً .

(انظر (٣-٦-٩) مثال ١٠ ، مثال ١١ فى نظرية الحلقات)

(٥) هل توجد أية أعداد ليست أولية r تقسم دائماً معاملات ذات الحدين $\binom{r}{s}$ ، حيث $1\le s\le r-1$ ؟

(٦) اوجد مولدات الزمر الضربية لـــ $GF(n)$ حيث

$n = 8, 9, 13, 17, 19, 23, 29, 31, 37, 41$ or 49

(٧) اعتبر الحقل $\mathbb{Z}_2(X)$. برهن على أن مونومورفيزم فوربينيس ليس دائماً أوتومورفيزماً .

(٨) ليكن φ هو أوتومورفيزم فوربينيس لـــ $GF(p^n)$. اوجد أصغر قيمة لـــ m ، $m > 0$ ، بحيث يكون φ هو راسم الوحدة .

(٩) إذا كانت n تقسم m ، فبرهن على أن $[GF(p^m):GF(p^n)] = \frac{m}{n}$.

(١٠) برهن على أن الحلقتين $\mathbb{Z}_3(X)/[X^2+X+2]$ ، $\mathbb{Z}_3(X)/[X^2+2X+2]$ متشاكلتان (أيزومورفيتان)

(١١) بدون حساب رتبة العنصر X وضح لماذا X مولد للزمرة الدائرية $(\mathbb{Z}_2(X)/[X^5+X^3+1])^*$

(١٢) ليكن m ، n عددين صحيحين موجبين ، m يقسم n . برهن على أنه لأى حقل F فإن $X^m - 1$ تقسم $X^n - 1$ فى $F[X]$.

(١٣)وضح بالرسم الاحتواءات التى تربط الحقول الجزئية من $GF(3^{18})$ ، $GF(2^{30})$.

(١٤) هل يمكنك أن تقارن رسم الاحتواءات التى تربط الحقول الجزئية من $GF(2^{30})$ بذلك الذى يوضح الاحتواءات التى تربط الحقول الجزئية من $GF(3^{30})$ ؟

(١٥) برهن على أن راسم فوربينيس

$$\varphi : GF(p^n) \to GF(p^n)$$
$$a \mapsto a^p$$

أوتومورفيزم من الرتبة n (أى أن φ^n هو راسم الوحدة)

(١٦) ليكن F حقلاً يتكون من 125 عنصراً ، $F^* = [a]$. برهن على أن $a^{62} = -1$

(١٧) ليكن K ، L حقلين جزئيين من $GF(p^n)$. إذا كان K يتألف من p^r عنصراً ، L يتألف من p^s عنصراً ، فكم عدد عناصر $K \cap L$ ؟

(١٨) إذا كان F حقلاً يتألف من 1024 عنصراً ، وكان $F^* = [a]$ ، فاسرد عناصر كل حقل جزئى من F .

(١٩) ليكن $\alpha, \beta \in (GF(81))^*$ ، بحيث إن رتبة $(\alpha) = 5$ ، رتبة $(\beta) = 16$.
برهن على أن $\alpha\beta$ مولد لـــ $(GF(81))^*$.

(٢٠) أوجد رتبة كل من الزمر الآتية :

(أ) $Aut(\mathbb{Q}(\sqrt[3]{2});\mathbb{Q})$

(ب) $Aut(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3});\mathbb{Q})$

(جـ) $Aut(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3});\mathbb{Q}(\sqrt[3]{2}))$

(٢١) ليكن F حقلاً ، وليكن α ، β جبريين على F ، درجة كثيرة الحدود الصغرى من α على F هى n . برهن على أن الراسم $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ المعرف كالآتى :

$$\psi_{\alpha,\beta}(c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \ldots + c_{n-1}\beta^{n-1}, c_i \in F$$

أيزومورفيزم من $F(\alpha)$ على $F(\beta)$ إذا كان وفقط إذا كان α ، β مترافقين على F .

(٢٢) الحقلان $\mathbb{Q}(\sqrt{2})$ ، $\mathbb{Q}(3+\sqrt{2})$ هما نفس الحقل . ليكن $\alpha = 3+\sqrt{2}$

(أ) اوجد مرافقاً β لـــ α على $\mathbb{Q}$ ، بحيث يكون $\beta \neq \alpha$

(ب) بالإشارة إلى (أ) قارن الأوتومورفيزم $\psi_{\sqrt{2},-\sqrt{2}}$ لـــ$\mathbb{Q}(\sqrt{2})$ مع الأوتومورفيزم $\psi_{\alpha,\beta}$

(٢٣) ليكن F حقلاً ، وليكن X غير محدد على F . عين جميع الأوتومورفيزمات لـــ $F(X)$ التى تترك F ثابتاً ، وذلك بتعيين كل قيمها على X .

(٢٤) التمرين (٢١) أعلاه يصف أيزومورفيزمات أساسية (basic isomorphisms) فى حالة α ، β جبريين مترافقين على F . هل يوجد أيزومورفيزم مشابه لـــ $F(\alpha)$ مع $F(\beta)$ فى حالة α ، β متساميين على F ؟

(٢٥) ليكن F حقلاً له المميز $p \neq 0$. اضرب مثالاً لبيان أن الراسم

$$\sigma_p : F \to F$$
$$a \mapsto a^p$$

لجميع $a \in F$ ليس بالضرورة أوتومورفيزماً إذا كان F ليس منتهياً .

(٢٦) برهن على أن $f \in F[X]$ ليس لها صفر مكرر إذا كان وفقط إذا كان f ، f' ليس لهما عامل غير ثابت مشترك في $F[X]$.

(٢٧) عين زمرة جالوا للامتداد $\mathbb{Q}(\sqrt{2},\sqrt{5}) \supset \mathbb{Q}$

(٢٨) ليكن $K \supset F$ امتداد حقل طبيعياً منتهياً ، وليكن $\alpha \in K$. **يعرف معيار** α **على** F (norm α over F) ونرمز له بالرمز $N_{K/F}(\alpha)$ كالآتي :

$$N_{K/F}(\alpha) := \prod_{\sigma \in Aut(K;F)} \sigma(\alpha)$$

بينما يعرف **أثر** α **على** F (trace α over F) كالآتي :

$$Tr_{K/F}(\alpha) := \sum_{\sigma \in Aut(K;F)} \sigma(\alpha)$$

والآن ليكن $K := \mathbb{Q}(\sqrt{2},\sqrt{3})$. احسب :

(أ) $N_{K/\mathbb{Q}}(\sqrt{2})$ (ب) $N_{K/\mathbb{Q}}(\sqrt{2}+\sqrt{3})$

(جـ) $N_{K/\mathbb{Q}}(\sqrt{6})$ (د) $N_{K/\mathbb{Q}}(2)$

(هـ) $Tr_{K/\mathbb{Q}}(\sqrt{2})$ (و) $Tr_{K/\mathbb{Q}}(\sqrt{2}+\sqrt{3})$

(ز) $Tr_{K/\mathbb{Q}}(\sqrt{6})$ (ح) $Tr_{K/\mathbb{Q}}(2)$

(٢٩) صف زمرة جالوا لكثيرة الحدود $X^4 - 5X^2 + 6 \in \mathbb{Q}[X]$ على $\mathbb{Q}$

(٣٠) صف زمرة جالوا لكثيرة الحدود $X^3 - 1 \in \mathbb{Q}[X]$ على $\mathbb{Q}$

(٣١) اعتبر الامتداد $\mathbb{Q}(\sqrt{3},\sqrt{5}) \supset \mathbb{Q}$

(أ) أية زمرة تشاكلها $Aut(\mathbb{Q}(\sqrt{3},\sqrt{5}),\mathbb{Q})$ ؟

(ب) ارسم شبكة الزمر الجزئية من $Aut(\mathbb{Q}(\sqrt{3},\sqrt{5}),\mathbb{Q})$ ، شبكة الحقول الجزئية من $\mathbb{Q}(\sqrt{3},\sqrt{5})$

(٣٢) ليكن $E = \mathbb{Q}(\sqrt{2},\sqrt{5})$ ، ما رتبة $Ord(Aut(E;\mathbb{Q}))$ ؟ ما رتبة $Ord(Aut(\mathbb{Q}(\sqrt{10});\mathbb{Q}))$ ؟

(٣٣) ليكن E حقل تشقيق كثيرة حدود على حقل F له المميز صفر . إذا كانت $Aut(E;F)$ زمرة إبدالية من الرتبة10 ، فارسم شبكة الحقول الجزئية للحقول بينE، F.

(إرشاد : استخدم شبكة الزمرة $\mathbb{Z}_{10}$)

(٣٤) ليكن F حقلاً له المميز صفر ، E حقل تشقيق لكثيرة حدود على F . إذا كانت $Aut(E;F)$ تتشاكل مع A_4 فبرهن على أنه لايوجد حقل جزئى K بحيث يكون $[K:F]=2$

(إرشاد : A_4 ليس لها زمرة جزئية من الرتبة 6)

(٣٥) إذا علم أن زمرة الأوتومورفيزمات لـــ $\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ تتشاكل مع $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$ ، فعين عدد الحقول الجزئية من $\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ التى درجة امتدادها على $\mathbb{Q}$ هى 4 .

(٣٦) برهن على أن زمرة جالوا لـــ X^3-3 على $\mathbb{Q}$ تتشاكل مع S_3 .

(٣٧) ليكن E هو حقل التشقيق لكثيرة حدود ما على حقل F له المميز صفر . إذا كان $[E:F]$ منتهيا ، فبرهن على أنه يوجد عدد منته فقط من الحقول بين E ، F .

(٣٨) إذا كانت w عدداً مركباً غير حقيقى بحيث إن $w^5=1$ ، وإذا كان φ أوتومورفيزماً لـــ $\mathbb{Q}(w)$ ينقل w إلى w^4 ، فاوجد الحقل الثابت لـــ $[\varphi]$.

(٣٩) عين زمرة حقل الأوتومورفيزمات لـــ $GF(4)$

(٤٠) ليكن $F \subset E$ امتداد حقل . برهن على أن زمرة أوتومورفيزمات E التى تثبت F هى بالفعل زمرة .

(٤١) ليكن $F \subset E$ امتداد حقل ، $H \subset Aut(E;F)$ زمرة جزئية . برهن على أن الحقل الثابت لـــ H هو بالفعل حقل .

(٤٢) اعتبر الحقل المنتهى $\mathbb{Z}_{11}$. اوجد الجذور البدائية الخمسية والجذور البدائية التربيعية للوحدة فى $\mathbb{Z}_{11}$. (ارشاد : انظر مثالى ٢٤ ، ٦٦ من أمثلة متنوعة ٢)

المُحتَوَيات

القسم الأول : نظرية الزمر

القسم الثانى : نظرية الحلقات

الثالث نظرية الحقول

الباب الاول

الباب الثانى